Über die Darstellbarkeit durch quadratische Formen im Körper der rationalen Funktionen einer Unbestimmten über dem Restklassenkörper *mod p*

Dissertation

zur Erlangung der Doktorwürde der naturwissenschaftlichen Fakultät der Universität Halle

Von

Herbert Rauter
(Tilsit)

(Tag der mündlichen Prüfung: 9. Juni 1926)

Druck von Friedr. Vieweg & Sohn Akt.-Ges., Braunschweig
1926

Über die Darstellbarkeit durch quadratische Formen im Körper der rationalen Funktionen einer Unbestimmten über dem Restklassenkörper *mod p*

Dissertation

zur Erlangung der Doktorwürde der naturwissenschaftlichen Fakultät der Universität Halle

Von

Herbert Rauter
(Tilsit)

(Tag der mündlichen Prüfung: 9. Juni 1926)

Druck von Friedr. Vieweg & Sohn Akt.-Ges., Braunschweig
1926

Referent: Prof. Dr. H. Hasse

Korreferent: Prof. Dr. Jung

R. UNIV.
BIBLIOTHEEK
LEIDEN

Inhaltsübersicht

Seite

Einleitung 5

§ 1. Der Körper K und die Henselschen Erweiterungskörper 6

§ 2. Vorbereitende Bemerkungen 11

A. Unäre Formen 15

§ 3. a) Darstellbarkeit der Null in $K(\mathfrak{p})$ durch binäre Formen 15

b) Darstellbarkeit der Null in K durch binäre Formen 16

c) Darstellbarkeit in K durch unäre Formen 17

B. Binäre Formen 17

§ 4. Darstellbarkeit der Null in $K(\mathfrak{p})$ durch ternäre Formen 17

§ 5. Das Symbol $\left\{\frac{\alpha_1, \alpha_2}{\mathfrak{p}}\right\}$ 18

§ 6. Darstellbarkeit in $K(\mathfrak{p})$ durch binäre Formen 26

§ 7. Darstellbarkeit der Null in K durch ternäre Formen 27

§ 8. Darstellbarkeit in K durch binäre Formen 29

C. Ternäre Formen 31

§ 9. Darstellbarkeit der Null in $K(\mathfrak{p})$ durch quaternäre Formen . . . 31

§ 10. Darstellbarkeit in $K(\mathfrak{p})$ durch ternäre Formen 33

§ 11. Darstellbarkeit der Null in K durch quaternäre Formen 34

§ 12. Darstellbarkeit in K durch ternäre Formen 36

D. n-äre Formen $(n \geq 4)$ 36

§ 13. Darstellbarkeit in $K(\mathfrak{p})$ durch n-äre Formen $(n \geq 4)$ 36

§ 14. Darstellbarkeit in K durch n-äre Formen $(n \geq 4)$ 37

§ 15. Zusammenfassung 38

Lebenslauf.

Ich, Herbert Leo Walter Rauter, bin als preußischer Staatsangehöriger evangelischen Bekenntnisses am 10. Januar 1899 als Sohn des Lehrers Albert Rauter in Kraplau, Kreis Osterode (Ostpreußen) geboren. Meinen ersten Unterricht genoß ich in der Dorfschule meines Vaters. Seit 1908 besuchte ich dann im Zusammenhang mit unserer Übersiedelung in die Stadt das Kaiser-Wilhelm-Gymnasium zu Osterode (Ostpreußen), wo ich am 3. März 1917 die Reifeprüfung ablegte. Ich trat dann beim Feldartillerieregiment 79 als Kriegsfreiwilliger ein und kam im Oktober desselben Jahres zum Lichtmeßtrupp 170 nach Rumänien an die Front, nahm an den Kämpfen in Rumänien und Palästina teil und kam hier September 1918 in englische Gefangenschaft, in der ich bis zum November 1919 blieb. Im Januar 1920 begann ich dann meine Studien an der Universität Königsberg, führte sie während drei Semestern in Berlin fort und beendete sie am 15. Mai 1924 durch die Staatsprüfung für das Lehramt an höheren Schulen in Königsberg. Meine Studien bezogen sich in erster Linie auf Mathematik, Physik, Geographie, Philosophie. Ich hörte während meines Studiums insbesondere die Herren Knopp, I. Schur, W. Fr. Meyer, Schmidt, Falckenberg, Rogosinski, Nernst, P. Volkmann, Kaufmann, Henning, Friedrichsen, Penck. Nach einem sich an die Staatsprüfung anschließenden Referendarjahr legte ich Ende März 1925 die pädagogische Prüfung in Königsberg ab und bin seit Beginn des Schuljahres 1925/26 in Tilsit als Studienassessor am Realgymnasium beschäftigt. Zwischendurch setzte ich meine wissenschaftlichen mathematischen Studien selbständig fort und empfing auf meine Bitte in bereitwilligstem Entgegenkommen von Herrn Prof. Hasse (Halle) außerordentlich reiche Anregungen zu selbständigen Forschungen auf zahlentheoretisch-algebraischen Gebieten, für die ich ihm zu großem Danke verpflichtet bin, darunter auch die Anregung zu dieser Dissertation.

Einleitung.

p sei eine ungerade Primzahl. Der Betrachtung zugrunde liegt dann der Körper K der rationalen Funktionen einer Unbestimmten über dem Restklassenkörper *mod* p, der also aus allen Funktionen

$$F(t) = \frac{a_m t^m + \cdots + a_0}{b_n t^n + \ldots + b_0}$$

besteht, wo die a_i und die b_i ganze rationale Zahlen bedeuten. Dieser Körper ist eingehend von Dedekind[1]) und in neuerer Zeit von Herrn Artin[2]) untersucht worden. In dieser Arbeit soll eine Frage beantwortet werden, die einer Anregung von Herrn Hasse entstammt und eng mit einem Problemkreis zusammenhängt, den er in einer Reihe von Arbeiten[3]) erschöpfend behandelt hat. Die Fragestellung, auf den vorliegenden Körper übertragen, lautet:

(I) Welches sind die notwendigen und hinreichenden Bedingungen dafür, daß eine Funktion μ aus K durch eine quadratische Form mit Koeffizienten aus K:

$$f = \sum_{i,k=1}^{n} \alpha_{ik} x_i x_k \quad (\alpha_{ik} = \alpha_{ki})$$

in K, d. h. durch Funktionen aus K für die Unbestimmten, darstellbar ist?

Herr Hasse vermutete nun, daß bei geeigneter Übertragung der „Henselschen Erweiterungskörper“ auf den vorliegenden Grundkörper die Antwort auf diese Frage ganz analog wie in seinen Arbeiten werde gegeben werden können, daß nämlich diese Darstellung dann

---

[1]) Dedekind, Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus, Journ. f. d. r. u. a. Math. **54**, 1ff., 1857.

[2]) E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen I. u. II, Math. Zeitschr. **19**, 153 ff., 1924. Im folgenden zitiert mit „Artin“.

[3]) Für diese Arbeit kommen in Frage: H. Hasse, Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen, Journ. f. d. r. u. a. Math. **152**, 129—148 und H. Hasse, Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper, Journ. f. d. r. u. a. Math. **153**, 113—130. Zitiert mit H. I. bzw. H. II.

und nur dann möglich ist, wenn sie in allen Henselschen Erweiterungskörpern gelingt. Wir werden die Richtigkeit dieser Vermutung bestätigen können.

---

§ 1. Der Körper K und die Henselschen Erweiterungskörper $K(\mathfrak{p})$.

Alle Funktionen der Form:

$$F(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0$$

heißen „ganze Funktionen“. Im folgenden schließen wir uns der Bezeichnungsweise Herrn Artins an und schreiben der Einfachheit halber alle Kongruenzen *mod p* als gewöhnliche Gleichungen. Ist also

$$F_1(t) = b_n t^n + b_{n-1} t^{n-1} + \cdots + b_0$$

eine zweite ganze Funktion, so soll

$$F(t) = F_1(t)$$

gleichbedeutend sein mit dem Bestehen der Kongruenzen:

$$a_\nu \equiv b_\nu \; mod \; p \quad (\nu = 0, 1, \ldots, n).$$

Im Körper K herrschen ganz ähnliche Gesetze wie im Körper der rationalen Zahlen. Insbesondere gilt ein Euklidischer Algorithmus für die Teilbarkeit der ganzen Funktionen[1]), woraus folgt, daß alle Ideale in K Hauptideale sind. Es folgt daraus auch die Gültigkeit der Gleichung

$$AF + BG = 1 \quad \ldots\ldots\ldots\ldots \quad (1)$$

für den Fall, daß F und G ganze Funktionen ohne gemeinsamen Teiler sind (A und B ganze Funktionen aus K), und die eindeutige Zerlegung jeder ganzen Funktion A aus K in ein Produkt von primären Primfunktionen P in der Form

$$A = a P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k} \quad \ldots\ldots\ldots\ldots \quad (2)$$

wo a eine „triviale Einheit *mod p*“, d. h. eine der Zahlen $1, 2 \ldots p-1$ bedeutet. Dabei wird eine ganze Funktion A aus K „primär“ genannt, wenn der Koeffizient der höchsten Potenz von $t \equiv 1 \; mod \; p$ ist.

Sämtliche ganzen Funktionen von K lassen sich in bekannter Weise nach einer (primären) Funktion A als Modul in p^α Funktionsklassen zusammenfassen, wenn mit α der Grad von A bezeichnet wird und in eine Klasse alle *mod A* kongruenten Funktionen geworfen werden. Ein vollständiges Repräsentantensystem dieser Klassen kann

[1]) Dedekind, a. a. O. S. 4.

stets in der Weise gegeben werden, daß die Repräsentanten kleineren Grad haben als A. Insbesondere können die zu einer (primären) Primfunktion P teilerfremden Restklassen dargestellt werden durch die $p^\pi - 1$ Potenzen

$$w_\mathfrak{p}^0, w_\mathfrak{p}^1, w_\mathfrak{p}^2, \ldots, w_\mathfrak{p}^{p^\pi - 2}$$

einer „primitiven Wurzel“ $w_\mathfrak{p}$[1]) *mod* P (π = Grad von P).

Für das Folgende ist es nun von höchster Wichtigkeit, daß sich die von Herrn Hensel herrührende Bildung der p-adischen Zahlen auf den vorliegenden Körper in sinngemäßer Weise übertragen läßt.

P sei eine (primäre) Primfunktion. Ist dann A eine beliebige ganze Funktion aus K, so besteht wegen der Gültigkeit des Euklidischen Algorithmus eine Gleichung der Form:

$$A = Q_0 P + R_0, \qquad \mathfrak{Gr}(R_0) < \mathfrak{Gr}(P).$$

Entsprechend gilt weiter:

$$\begin{aligned} Q_0 &= Q_1 P + R_1, & \mathfrak{Gr}(R_1) &< \mathfrak{Gr}(P) \\ Q_1 &= Q_2 P + R_2, & \mathfrak{Gr}(R_2) &< \mathfrak{Gr}(P) \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ Q_{n-2} &= Q_{n-1} P + R_{n-1}, & \mathfrak{Gr}(R_{n-1}) &< \mathfrak{Gr}(P) \end{aligned}$$

Diese Gleichungskette muß schließlich abbrechen, da die Grade von A, Q_0, $Q_1 \ldots Q_k \ldots$ abnehmen. Setzt man nun in der ersten Gleichung für Q_0 den Ausdruck der zweiten, dann für Q_1 den Ausdruck der dritten usw., schließlich für Q_{n-2} den Ausdruck der letzten Gleichung ein, so erhält man eine Darstellung von A nach aufsteigenden Potenzen von P:

$$A = R_0 + R_1 P + R_2 P^2 + \cdots + R_n P^n, \quad \ldots\ldots \quad (3)$$

eine „P-adische Funktion“, wenn wir noch zweckmäßig $Q_{n-1} = R_n$ setzen [denn wegen des Abbrechens der Reihe ist auch $\mathfrak{Gr}(Q_{n-1}) < \mathfrak{Gr}(P)$]. Die R_i können dabei zum Teil auch gleich 0 sein. Es sei R_k die erste Funktion aus der Reihe der R_i, die nicht verschwindet, dann würde A die folgende P-adische Darstellung zulassen:

$$A = R_k P^k + R_{k+1} P^{k+1} + \cdots + R_n P^n \quad \ldots\ldots \quad (3')$$

Die Zahl k soll die „Ordnungszahl“ von A im Bereiche der P-adischen Funktionen heißen.

Man erkennt nun leicht, daß sich von hier aus das System der P-adischen Funktionen genau in derselben Weise aufbauen läßt, wie es Herr Hensel für die p-adischen bzw. π-adischen algebraischen

---

[1]) Dedekind, a. a. O. S. 15

Zahlen getan hat[1]). Wir begnügen uns hier mit den wesentlichsten und für das Folgende wichtigsten Schritten.

Zunächst nennen wir eine Funktion A in der Form (3′) eine „Einheit“ für den Bereich von P, wenn sie die Ordnungszahl 0 hat. Ferner muß auch hier der Unterschied zwischen „reduzierten“ und nicht-reduzierten P-adischen Funktionen gemacht werden. In der nicht-reduzierten Form können die Koeffizienten der Potenzen von P beliebige ganze Funktionen sein. „Reduziert“ werden wir die Darstellung von A dann nennen, wenn entweder der Grad der Koeffizienten durchgehend kleiner ist als der von P, oder wenn sie, soweit sie $\not\equiv 0 \ mod\ P$ sind, als Potenzen von $w_\mathfrak{p}$ dargestellt sind. Es gilt auch hier der Satz, daß jede P-adische Funktion einer und nur einer reduzierten P-adischen Funktion gleich ist. Wir werden im folgenden daher die P-adischen Funktionen immer in der reduzierten Form gegeben annehmen. Ist

$$B = R_0' + R_1' P + \cdots + R_n' P^n$$

eine zweite P-adische Funktion, so wird die Addition von A und B erklärt durch:

$$A + B = (R_0 + R_0') + (R_1 + R_1') P + \cdots + (R_n + R_n') P^n \quad . \quad . \quad . \quad (4)$$

Im allgemeinen wird die Summe in der nicht-reduzierten Form vorliegen.

Die Subtraktion wird als Umkehrung der Addition eingeführt und führt genau wie bei Herrn Hensel zu einer Erweiterung des bisherigen Bereiches der P-adischen Funktionen, wenn unbeschränkte Ausführbarkeit der Subtraktion gefordert wird[2]):

Unter einer P-adischen Funktion ist jede Reihe:

$$R_0 + R_1 P + R_2 P^2 + \cdots$$

mit $mod\ P$ reduzierten Koeffizienten zu verstehen, mag sie nun abbrechen oder nicht, wenn eine Vorschrift existiert, nach welcher ihre Koeffizienten so weit berechnet werden können, als man nur immer will.

Die Multiplikation zweier P-adischer Funktionen A und B wird analog der Cauchyschen Produktregel für konvergente Reihen erklärt durch:

$$A\,B = R_0 R_0' + (R_0 R_1' + R_0' R_1) P + \cdots \quad . \quad . \quad . \quad . \quad (5)$$

---

[1]) K. Hensel, Theorie der algebraischen Zahlen I, 1908, 1. u. 2. Kap. — Derselbe, Zahlentheorie, 1913.

[2]) Vgl. Hensel, Algebraische Zahlen, S. 16.

Auch das Produkt wird im allgemeinen zunächst in der nicht-reduzierten Form errechnet werden.

Eine nochmalige Erweiterung unseres Funktionsgebiets wird notwendig, wenn wir zur Definition der Division schreiten. Sie wird natürlich erklärt als Umkehrung der Multiplikation. Sind zunächst A und B P-adische Einheiten, ist also R_0 und $R'_0 \neq 0$, so berechnet sich der Quotient $\frac{A}{B}$ zu

$$\frac{A}{B} = C = R''_0 + R''_1 P + R''_2 P^2 + \cdots, \quad \ldots\ldots (6)$$

wo die Koeffizienten R''_0, R''_1, R''_2 ... die Werte

$$R''_0 = \frac{R_0}{R'_0}, \quad R''_1 = \frac{R_1 R'_0 - R_0 R'_1}{R'^2_0} \text{ usw.} \quad \ldots\ldots (6')$$

annehmen[1]). Soll nun auch die Division im Bereiche der P-adischen Funktionen unbeschränkt ausführbar sein, so wird folgende Definition notwendig:

Definition: Eine gebrochene Funktion $\frac{M}{N}$ aus K (M und N werden dabei als teilerfremde Funktionen vorausgesetzt), soll „*mod P* ganz“ heißen, wenn N zu P teilerfremd, also durch P nicht teilbar ist.

Dementsprechend erfährt dann auch der Begriff der Teilbarkeit eine Erweiterung:

Sind A und B zwei *mod P* ganze Funktionen aus K, so heißt A durch B *mod P* teilbar, wenn eine dritte *mod P* ganze Funktion Q existiert, so daß

$$A = Q B$$

wird.

Man zeigt dann leicht, daß auch jede nur *mod P* ganze Funktion einer und nur einer Funktion eines *mod P* reduzierten Restklassensystems kongruent ist. Denn da N und P teilerfremd sind, folgt das Bestehen einer Gleichung

$$A N + B P = 1,$$

aus der sofort die andere:

$$A' N + B' P = M,$$

gefolgert werden kann. (A, B, A', B' ganze Funktionen aus K.) Dividieren wir die letzte Gleichung durch N, so ergibt sich:

$$A' + \frac{B'}{N} P = \frac{M}{N},$$

[1]) Vgl. K. Hensel, Algebraische Zahlen, S. 30.

wo $\frac{B'}{N}$ offenbar *mod* P ganz ist. Auf Grund unseres neuen Teilbarkeitsbegriffs können wir offenbar diese letzte Gleichung folgendermaßen als Kongruenz schreiben:

$$\frac{M}{N} \equiv A' \bmod P,$$

so daß $\frac{M}{N}$ einer ganzen Funktion A' aus K *mod* P kongruent wird, woraus dann leicht die Behauptung folgt.

Jetzt sind wir in der Lage, den Quotienten zweier P-adischen Einheiten mit den Koeffizienten (6′) in die reduzierte Form einer P-adischen Funktion überzuführen, denn diese letzteren können ja durch Repräsentanten eines reduzierten Restklassensystems bzw. durch 0 ersetzt werden.

Die Division zweier beliebiger P-adischer Funktionen kann immer zurückgeführt werden auf die Division zweier P-adischer Einheiten. Denn liegt A in der Form (3′) vor, so kann es auch geschrieben werden:

$$A = P^k(R_k + R_{k+1} P + \cdots) = P^k E,$$

wo E eine P-adische Einheit bedeuten soll. Ebenso läßt sich B immer in der Form

$$B = P^{k'} E'$$

annehmen. Dann nimmt aber der Quotient von A und B die Gestalt an:

$$C = \frac{A}{B} = P^{k-k'} \frac{E}{E'} = P^{k-k'} E'',$$

da, wie wir vorher gesehen haben, der Quotient zweier Einheiten *mod* P wieder eine Einheit *mod* P ist. Allerdings können jetzt im Quotienten C negative Potenzen von P auftreten, so daß die allgemeinste P-adische Funktion in der Form anzunehmen wäre:

$$A = R_k P^k + R_{k+1} P^{k+1} + \cdots \quad (k \gtrless 0) \quad . \quad . \quad . \quad . \quad . \quad (7)$$

Hat A negative Ordnungszahl, so werden wir es als eine gebrochene P-adische Funktion bezeichnen.

Die Gesamtheit aller ganzen und gebrochenen P-adischen Funktionen bildet offenbar einen Körper, den wir hinfort immer durch $K(\mathfrak{p})$ bezeichnen werden. Dabei bedeutet $\mathfrak{p} = (P)$ das durch die Primfunktion P erzeugte Primideal. Wir werden häufig auch von $\mathfrak{p}$-adischen statt von P-adischen Funktionen sprechen.

So gehört also zu jeder Primfunktion P aus K ein durch sie eindeutig bestimmter Körper $K(\mathfrak{p})$. Diese in unendlicher Anzahl vorhandenen Körper $K(\mathfrak{p})$ vermehren wir noch um einen weiteren, den wir durch $K(\mathfrak{p}_\infty)$ bezeichnen wollen. Er entspricht dem Körper $K(p_\infty)$ bei den rationalen Zahlen. Wir definieren ihn als die Gesamtheit aller endlichen und unendlichen Reihen:

$$\alpha = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_0 + a_{-1} t^{-1} + \cdots \quad (a_n \neq 0) \quad . \quad . \quad . \quad (8)$$

in denen nur endlich viele positive Potenzen von t vorkommen und die a_i irgendwelche Einheiten *mod* p oder 0 bedeuten. Man sieht sofort, daß $K(\mathfrak{p}_\infty)$ den Grundkörper K als Teilkörper enthält.

§ 2. Vorbereitende Bemerkungen.

Das Ziel unserer Arbeit wird der Beweis des Fundamentalsatzes (II) sein:

(II) Damit eine Funktion μ aus K durch eine n-äre quadratische Form f mit Koeffizienten aus K in K darstellbar ist, ist notwendig und hinreichend, daß μ durch f in allen $K(\mathfrak{p})$ einschließlich $K(\mathfrak{p}_\infty)$ darstellbar ist.

Die in (I) auf S. 5 gestellte Hauptfrage wird damit zurückgeführt auf die entsprechende für die einzelnen $K(\mathfrak{p})$.

Durch die Einführung der $\mathfrak{p}$-adischen Funktionen gelingt es nun, für die Inangriffnahme des Problems eine ähnlich günstige Ausgangsbasis zu schaffen, wie sie Herrn Hasse im Körper der rationalen bzw. algebraischen Zahlen zur Verfügung stand. Auch hier liegt jeder Funktion $\mu \neq 0$ aus K bzw. $K(\mathfrak{p})$ eine von allen Quadraten des betreffenden Körpers befreite, eindeutig bestimmte reduzierte Funktion zugrunde, die wir ihren (quadratischen) Kern in K bzw. in $K(\mathfrak{p})$ nennen wollen. Nur dieser Kern ist für die Darstellbarkeit von μ in K bzw. in $K(\mathfrak{p})$ maßgebend, da jeder in μ enthaltene quadratische Faktor durch Division in die Variablen der Form gezogen werden kann.

Die Kerne von μ in K, die wir hinfort durch $[\mu]$ bezeichnen wollen, können wir, wie man sich leicht klarmacht, als ganze Funktionen in K von der Form

$$[\mu] = g^a P_1 P_2 \ldots P_m \quad (a = 0 \text{ oder } 1) \quad . \quad . \quad . \quad . \quad . \quad . \quad (9)$$

annehmen, wo g eine in Zukunft festgehaltene primitive Wurzel von p, $P_1, P_2, \ldots, P_m$ aber voneinander verschiedene Primfunktionen bedeuten.

Für den Körper $K(\mathfrak{p}_\infty)$ ist unsere Aufgabe, wenn auch nicht für den vorliegenden Zweck, schon von Herrn Artin a. a. O. in § 3 gelöst worden. Liegt die Funktion in $K(\mathfrak{p}_\infty)$

$$\begin{aligned}\mu &= a_n t^n + a_{n-1} t^{n-1} + \cdots \quad (a_n \neq 0)\\ &= a_n t^n \left(1 + \frac{a_{n-1}}{a_n} t^{-1} + \cdots\right)\\ &= a_n t^n (1 + \lambda)\end{aligned}$$

vor, so gilt nach dem dortigen Beweise eine Gleichung

$$1 + \lambda = \left(\sum_{\nu=1}^{\infty} \binom{1/2}{\nu} \lambda^\nu\right)^2,$$

wo das Quadrat rechts nach der Cauchyschen Produktregel berechnet wird, und $\binom{1/2}{\nu}$ wegen $p \neq 2$ eine *mod p* ganze rationale Zahl ist, d. h. jeder Ausdruck der Form $1 + \lambda$ ist in $K(\mathfrak{p}_\infty)$ ein volles Quadrat. Setzen wir nun noch $a_n = g^{2k+a}$, $t^n = t^{2l+b}$, wo a bzw. b gleich 0 oder 1 ist, je nachdem der Index von a_n bzw. der Grad n von t gerade oder ungerade ist, so folgt als Kern von μ in $K(\mathfrak{p}_\infty)$, den wir durch $\mu_{\mathfrak{p}_\infty}$ bezeichnen wollen, der Ausdruck:

$$\mu_{\mathfrak{p}_\infty} = g^a t^b \quad (a, b \text{ gleich } 0 \text{ oder } 1). \quad \ldots\ldots \quad (10)$$

Die Funktionen von $K(\mathfrak{p}_\infty)$ zerfallen danach in bezug auf ihren quadratischen Charakter in vier Funktionsklassen, wobei in eine Klasse alle die Funktionen geworfen werden, die denselben Kern in $K(\mathfrak{p}_\infty)$ besitzen. Alle und nur die Funktionen, die den Kern 1 haben, sind Quadrate in $K(\mathfrak{p})$.

Auf eine ähnliche Weise gelingt es nun auch, die Kerne in den $K(\mathfrak{p})$ zu finden. Ist nämlich

$$\begin{aligned}\mu &= \alpha_n P^n + \alpha_{n+1} P^{n+1} + \cdots \quad (\alpha_n \neq 0)\\ &= \alpha_n P^n \left(1 + \frac{\alpha_{n+1}}{\alpha_n} P + \cdots\right)\\ &= \alpha_n P^n (1 + \lambda)\end{aligned}$$

irgend eine P-adische Funktion, so zeigt man leicht, daß auch hier der Ausdruck $1 + \lambda$ ein volles Quadrat in $K(\mathfrak{p})$ darstellt. Man braucht nämlich in dem vorher erwähnten Beweise von Herrn Artin nur formal $a_n, a_{n-1}, \ldots$ bzw. durch $\alpha_n, \alpha_{n+1}, \ldots$ und t^{-1} durch P zu ersetzen, um einzusehen, daß auch hier

$$1 + \lambda = \left(\sum_{\nu=0}^{\infty} \binom{1/2}{\nu} \lambda^\nu\right)^2$$

ist, wo auf der rechten Seite das Quadrat einer auf Grund der Produktregel (5) wohlbestimmten P-adischen Funktion steht. Setzt man

noch, was gestattet ist, α_n als Potenz einer primitiven Wurzel $w_\mathfrak{p}$ von P voraus, $\alpha_n = w_\mathfrak{p}^{2k+a}$, $P^n = P^{2l+b}$, wo a bzw. b gleich 0 oder 1, je nachdem der Index von α_n bzw. die Ordnungszahl von μ gerade oder ungerade ist, so erkennt man auch hier, daß man als Kern in $K(\mathfrak{p})$, der durch $\mu_\mathfrak{p}$ bezeichnet werde, einen der Ausdrücke

$$\mu_\mathfrak{p} = w_\mathfrak{p}^a P^b \ (a, b \text{ gleich } 0 \text{ oder } 1) \quad . \quad . \quad . \quad . \quad . \quad . \quad (11)$$

erhält. Für die Einteilung der Funktionen von $K(\mathfrak{p})$ in Klassen, ihrem quadratischen Charakter nach, gilt analoges, wie es für $K(\mathfrak{p}_\infty)$ gesagt wurde.

Quadratische Formen, die durch lineare Substitutionen mit Koeffizienten aus K bzw. $K(\mathfrak{p})$ von nicht verschwindender Determinante zusammenhängen, werden auch hier in K bzw. $K(\mathfrak{p})$ äquivalent genannt. In K bzw. in $K(\mathfrak{p})$ äquivalente Formen stellen dieselben Funktionen in K bzw. in $K(\mathfrak{p})$ dar. Insbesondere gilt dies auch für die Darstellbarkeit der Null.

Es folgt nun auch hier mit Hilfe eines Beweises, der formal ebenso verläuft wie bei Hensel (Zahlentheorie Kap. XII, § 2), daß jede quadratische Form einer Anzahl reiner Formen, d. h. Formen

$$F = \sum_{i=1}^{n} A_i x_i^2,$$

mit nur rein quadratischen Gliedern in K bzw. in den $K(\mathfrak{p})$ äquivalent ist. Bei der Aufstellung der Darstellbarkeitskriterien in K bzw. in den $K(\mathfrak{p})$ dürfen wir uns daher nach dem vorher Bemerkten auf solche reine Formen oder noch einfacher auf die in K bzw. in den $K(\mathfrak{p})$ äquivalenten Formen

$$f = \sum_{i=1}^{n} \alpha_i x_i^2 \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad (12)$$

beschränken, wo die α_i die quadratischen Kerne der A_i in K bzw. $K(\mathfrak{p})$ sind. Derartige Formen f wollen wir reine Kernformen nennen. Für das Folgende ist wichtig, daß die Darstellbarkeit der Null auch gegen Multiplikation der Form mit von Null verschiedenen Funktionen invariant ist, so daß z. B. durch Multiplikation von f mit α_1 bzw. $-\alpha_1$ und nachherige einfache Transformation der erste Koeffizient von f immer gleich $+1$ oder -1 angenommen werden kann.

Die Diskriminante einer quadratischen Form, d. h. die Determinante $\Delta = |\alpha_{ik}|$ ihres Koeffizientensystems, setzen wir durchweg von Null verschieden voraus. Da sich diese Determinante bei Transformation der Form in K bzw. $K(\mathfrak{p})$ bekanntlich nur mit einem Quadrat

aus K bzw. $K(\mathfrak{p})$ multipliziert, haben in K bzw. $K(\mathfrak{p})$ äquivalente Formen denselben Diskriminantenkern in K bzw. $K(\mathfrak{p})$. Wir wollen den Diskriminantenkern in K in Zukunft immer mit δ, den in $K(\mathfrak{p})$ bzw. $K(\mathfrak{p}_\infty)$ mit $\delta_\mathfrak{p}$ bzw. $\delta_{\mathfrak{p}_\infty}$ bezeichnen. Die einzelnen $\mathfrak{p}$-adischen Diskriminantenkerne $\delta_\mathfrak{p}$ ein und derselben Form aus K sind zugleich die $\mathfrak{p}$-adischen Kerne des Diskriminantenkerns δ aus K. Wir haben daher ein Recht, von den Invarianten δ bzw. $\delta_\mathfrak{p}$ einer Form zu sprechen.

Wichtig ist noch die Bemerkung, daß für ein gerades n offenbar δ bzw. $\delta_\mathfrak{p}$ gegen Multiplikation der Form mit von Null verschiedenen Funktionen aus K bzw. $K(\mathfrak{p})$ invariant ist.

Besteht für eine reine Form in K bzw. $K(\mathfrak{p})$ eine nicht identische Gleichung $f = 0$, so gilt auch in unserem Körper, daß diese Gleichung dann auch mit sämtlich von Null verschiedenen Variablen besteht [1]).

Auf Grund dieser Tatsache gelingt es, das vorliegende Problem mit denselben Methoden wie in H. I anzugreifen. Unser Problem läßt sich auf die beiden Hauptaufgaben reduzieren:

(III) a) Aufstellung der Darstellbarkeitskriterien für die $K(\mathfrak{p})$;

b) Nachweis des Fundamentalsatzes (II).

Der Weg dazu wird nach den vorigen Bemerkungen geebnet durch:

(IV) Damit $\mu \neq 0$ in K bzw. $K(\mathfrak{p})$ durch eine beliebige n-äre Form $f(x_1 \ldots x_n)$ darstellbar ist, ist notwendig und hinreichend, daß die Null in K bzw. $K(\mathfrak{p})$ durch die $(n+1)$-äre Form

$$F = f(x_1, \ldots, x_n) - \mu x^2$$

darstellbar ist.

Durch (IV) reduzieren sich die beiden Hauptaufgaben (III) auf:

(V) a) Aufstellung der Darstellbarkeitskriterien für $\mu = 0$ in $K(\mathfrak{p})$ durch $(n+1)$-äre-Formen;

b) Nachweis des Fundamentalsatzes (II) für $\mu = 0$ und $(n+1)$-äre Formen.

Sehr wichtig ist noch die Bemerkung, daß f sicher dann die Null in K bzw. den $K(\mathfrak{p})$ darstellt, wenn dies nur für irgend eine binäre oder höhere Teilform von f der Fall ist, unter Teilform jede Teilsumme von Gliedern von f verstanden, die mit den übrigen Gliedern keine Variable gemeinsam haben.

---

[1]) Beweisführung wie in H. I, S. 133, Anm. 1.

A. Unäre Formen.

§ 3.

a) Darstellbarkeit der Null in $K(\mathfrak{p})$ durch binäre Formen.

1. $\mathfrak{p} = (P)$.

Liegt die binäre quadratische Form

$$f(x_1, x_2) = \alpha_1 x_1^2 + \alpha_2 x_2^2$$

vor, in der α_1 und α_2 $\mathfrak{p}$-adische Kerne bedeuten, so kann f nach § 2 immer auf die für die vorliegende Aufgabe gleichwertige Normalform

$$f_0(x_1, x_2) = x_1'^2 + \delta_\mathfrak{p} x_2'^2 \quad \ldots\ldots\ldots \quad (12')$$

gebracht angenommen werden. Aus $f_0 = 0$ folgt dann

$$\left(\frac{x_1'}{x_2'}\right)^2 = -\delta_\mathfrak{p} \quad \ldots\ldots\ldots\ldots \quad (12'')$$

d. h. $-\delta_\mathfrak{p}$ muß $\mathfrak{p}$-adisches Quadrat sein. Wir führen nun für eine beliebige $\mathfrak{p}$-adische Funktion α das Symbol

$$\left[\frac{\alpha}{P}\right] = \left[\frac{\alpha}{\mathfrak{p}}\right] = [(-1)^a, (-1)^b] \quad \ldots\ldots\ldots \quad (13)$$

ein, wenn $\alpha_\mathfrak{p} = w_\mathfrak{p}^a P^b$, und setzen es nur dann gleich $+1$, wenn beide in der eckigen Klammer enthaltenen Potenzen von -1 gleich $+1$ werden, in allen übrigen Fällen gleich -1. Man erkennt, daß $\left[\frac{\alpha}{\mathfrak{p}}\right]$ dann und nur dann gleich $+1$ wird, wenn α Quadrat in $K(\mathfrak{p})$ ist, ferner die Übereinstimmung mit dem von Herrn Artin a. a. O. S. 170 eingeführten Symbol $\left[\frac{\alpha}{P}\right]$. Außerdem genügt das Symbol der Gleichung

$$\left[\frac{\alpha_1}{\mathfrak{p}}\right]\left[\frac{\alpha_2}{\mathfrak{p}}\right] = \left[\frac{\alpha_1 \alpha_2}{\mathfrak{p}}\right] \quad \ldots\ldots\ldots\ldots \quad (14)$$

Aus der zuletzt erzielten Gleichung (12'') folgt dann als notwendige und hinreichende Bedingung für die Darstellbarkeit der Null durch f_0 und damit durch f in $K(\mathfrak{p})$ die Gleichung

$$\left[\frac{-\delta_\mathfrak{p}}{\mathfrak{p}}\right] = +1 \quad \ldots\ldots\ldots\ldots \quad (15)$$

Da $\left[\frac{-\delta_\mathfrak{p}}{\mathfrak{p}}\right] = \left[\frac{-1}{\mathfrak{p}}\right]\left[\frac{\delta_\mathfrak{p}}{\mathfrak{p}}\right]$ und nach dem Ergänzungssatz zum quadratischen Reziprozitätsgesetz[1]) $\left[\frac{-1}{\mathfrak{p}}\right] = (-1)^{\frac{p-1}{2}\cdot\pi}$ ist, wenn π

[1]) Artin, § 15.

den Grad von P bedeutet, so kann der obigen Darstellbarkeitsbedingung auch die Form

$$\left[\frac{\delta_\mathfrak{p}}{\mathfrak{p}}\right] = (-1)^{\frac{p-1}{2}\cdot\pi} \quad \ldots\ldots\ldots\ldots \quad (15')$$

gegeben werden.

2. $\mathfrak{p} = \mathfrak{p}_\infty$.

Wie vorher folgert man aus $f = 0$ die Gleichung

$$\left(\frac{x_1'}{x_2'}\right)^2 = -\delta_{\mathfrak{p}_\infty} \quad \ldots\ldots\ldots\ldots \quad (16)$$

Man übersieht nun sofort, daß man das in $K(\mathfrak{p})$ eingeführte Symbol $\left[\frac{\alpha}{\mathfrak{p}}\right]$ unmittelbar auf $K(\mathfrak{p}_\infty)$ in der Form übertragen kann:

$$\left[\frac{\alpha}{\mathfrak{p}_\infty}\right] = \left[(-1)^a,\ (-1)^b\right] \quad \ldots\ldots\ldots \quad (13')$$

wenn $\alpha_{\mathfrak{p}_\infty} = g^a t^b$ gesetzt wird. Auch hier wird das Symbol gleich $+1$ oder -1 gesetzt, je nachdem beide Potenzen von -1 zugleich gleich $+1$ oder nicht sind. Auch hier ist $\left[\frac{\alpha}{\mathfrak{p}_\infty}\right] = +1$ dann und nur dann, wenn α Quadrat in $K(\mathfrak{p}_\infty)$ ist. Analog wie bei 1. folgt daher als Darstellbarkeitsbedingung in $K(\mathfrak{p}_\infty)$:

$$\left[\frac{-\delta_{\mathfrak{p}_\infty}}{\mathfrak{p}_\infty}\right] = +1 \quad \ldots\ldots\ldots\ldots \quad (15'')$$

Damit ist bewiesen der

Satz 1: Eine binäre Form stellt die Null dann und nur dann in $K(\mathfrak{p})$ [einschließlich $K(\mathfrak{p}_\infty)$] dar, wenn ihre Invariante $\delta_\mathfrak{p}$ der Bedingung $\left[\frac{-\delta_\mathfrak{p}}{\mathfrak{p}}\right] = +1$ genügt.

b) Darstellbarkeit der Null in K durch binäre Formen.

Wir können $f(x_1, x_2)$ gleich in der normierten Form

$$f = x_1^2 + \delta x_2^2$$

annehmen. Aus $f = 0$ folgt dann

$$\left(\frac{x_1}{x_2}\right)^2 = -\delta,$$

d. h. es muß $-\delta$ Quadrat in K sein.

Nun ist allgemein ein Quadrat in K natürlich auch in allen $K(\mathfrak{p})$ einschl. $\mathfrak{p} = \mathfrak{p}_\infty$ Quadrat. Umgekehrt ist aber auch eine Funktion

aus K, die in allen $K(\mathfrak{p})$ einschließlich $\mathfrak{p} = \mathfrak{p}_\infty$ Quadrat ist (d. h. zur $\mathfrak{p}$-adischen Funktionsklasse von $+1$ gehört), Quadrat in K. Denn eine solche Funktion hat für jedes P gerade Ordnungszahl, ist also durch keine Primfunktion P in ungerader Potenz teilbar und kann außerdem, wenn wir sie in der gekürzten Form

$$g^a \frac{P_1^{2m_1} P_2^{2m_2} \dots P_k^{2m_k}}{Q_1^{2n_1} \dots Q_l^{2n_l}} \quad (P_r, Q_s \text{ voneinander verschiedene Primfunktionen})$$

schreiben, keinen ungeraden Exponenten a von g besitzen, da sie auch in $K(\mathfrak{p}_\infty)$ Quadrat sein soll. Hieraus folgt sofort die Gültigkeit des Fundamentalsatzes (II) für $\mu = 0$ und $n = 2$:

Satz 2: Eine binäre Form stellt die Null dann und nur dann in K dar, wenn sie sie in allen $K(\mathfrak{p})$ darstellt, d. h. wenn ihre Invariante δ der Bedingung $\left[\frac{-\delta}{\mathfrak{p}}\right] \equiv +1$ genügt.

Dabei soll das Zeichen $\equiv$ hier und an allen ähnlichen Stellen „für alle $\mathfrak{p}$ einschl. $\mathfrak{p}_\infty$ gleich“ bedeuten.

c) Darstellbarkeit in K durch unäre Formen.

Die vollständige Antwort auf die Fragestellung (I) für unäre Formen wird mittels des Satzes 2 durch die in (IV) dargestellte Schlußweise gegeben, kann aber auch unmittelbar erkannt werden. Sie lautet:

Satz 3: Eine Funktion $\mu \neq 0$ aus K ist dann und nur dann durch eine unäre Form der Invariante δ darstellbar, wenn sie der Bedingung $\left[\frac{\mu}{\mathfrak{p}}\right] = \left[\frac{\delta}{\mathfrak{p}}\right]$ genügt, d. h. wenn μ den Kern δ in K hat.

B. Binäre Formen.

§ 4. Darstellbarkeit der Null in $K(\mathfrak{p})$ durch ternäre Formen.

Nach den Erörterungen in § 2 sind wir berechtigt, die ternäre Form von vornherein in der normierten Gestalt

$$f_0(x_0, x_1, x_2) = -x_0^2 + \alpha_1 x_1^2 + \alpha_2 x_2^2$$

anzunehmen, wo α_1 und α_2 $\mathfrak{p}$-adische Kerne sind. Wir führen nun im folgenden in Analogie zum Hilbertschen Symbol das Zeichen $\left\{\frac{\alpha_1, \alpha_2}{\mathfrak{p}}\right\}$ (einschließlich $\mathfrak{p} = \mathfrak{p}_\infty$) ein und setzen

$$\left\{\frac{\alpha_1, \alpha_2}{\mathfrak{p}}\right\} = +1 \text{ oder } -1,$$

je nachdem durch die Form f_0 die Null in $K(\mathfrak{p})$ dargestellt werden kann oder nicht, oder, wie wir im Anschluß an die Ausdrucksweise von Herrn Hensel sagen wollen, je nachdem $\mathfrak{p}$ bzw. $\mathfrak{p}_\infty$ ein Teiler der Form f_0 ist oder nicht. Für den Wert des Symbols ist es, wie man leicht sieht, belanglos, ob zu α_1 oder α_2 irgendwelche quadratische Faktoren hinzutreten. Ist allgemeiner der vorliegenden ternären Form die reine Kernform

$$f_0(x_1, x_2, x_3) = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2$$

in $K(\mathfrak{p})$ äquivalent, so folgt sofort aus der Definition des Symbols der

Satz 4: Eine ternäre Form f stellt die Null in $K(\mathfrak{p})$ dann und nur dann dar, wenn für irgend eine ihr äquivalente reine Kernform

$$f_0(x_1, x_2, x_3) = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2$$

die Einheit

$$\hat{c}_\mathfrak{p} = \hat{c}_\mathfrak{p}(f_0) = \left\{\frac{-\alpha_1\alpha_2, -\alpha_1\alpha_3}{\mathfrak{p}}\right\} \quad \cdots\cdots (17)$$

den Wert $+1$ hat.

$\hat{c}_\mathfrak{p}(f_0)$ ist demnach, ebenso wie die Darstellbarkeit der Null in $K(\mathfrak{p})$, eine Invariante gegen $\mathfrak{p}$-adische Transformation und Multiplikation von f und kann als $\hat{c}_\mathfrak{p}(f)$ bezeichnet werden. Zu jeder ternären Form f in K gehört also ein über alle Primideale $\mathfrak{p}$ erstrecktes System $(\hat{c}_\mathfrak{p})$, dessen einzelne Einheiten über die Darstellbarkeit der Null in den einzelnen $K(\mathfrak{p})$ entscheiden. Dies System $[\hat{c}_\mathfrak{p}(f)]$ in seiner Gesamtheit ist invariant gegen Transformation und Multiplikation von f in K.

§ 5. Das Symbol $\left\{\frac{\alpha_1, \alpha_2}{\mathfrak{p}}\right\}$.

Unsere nächste Aufgabe wird es sein müssen, die Auswertungsgesetze dieses Symbols aufzusuchen. Aus der Definition folgt als erstes Gesetz unmittelbar das

$$\text{Vertauschungsgesetz: } \left\{\frac{\alpha_1, \alpha_2}{\mathfrak{p}}\right\} = \left\{\frac{\alpha_2, \alpha_1}{\mathfrak{p}}\right\} \quad \cdots (18)$$

Wie schon in § 4 bemerkt, ist es für den Wert des Symbols belanglos, ob zu α_1 und α_2 quadratische Faktoren in $K(\mathfrak{p})$ hinzutreten oder nicht. Wir können daher α_1 und α_2 gleich als $\mathfrak{p}$-adische Kerne annehmen.

Es sei zunächst $\mathfrak{p} = (P)$. Außerdem sei weder α_1 noch α_2 durch P teilbar. Aus

$$f(x_0, x_1, x_2) = -x_0^2 + w_\mathfrak{p}^{b_1} x_1^2 + w_\mathfrak{p}^{b_2} x_2^2 = 0$$

folgt dann

$$x_0^2 = w_{\mathfrak{p}}^{a_1} x_1^2 + w_{\mathfrak{p}}^{a_2} x_2^2, \ (a_1, a_2 \text{ gleich } 0 \text{ oder } 1) \ \ldots \ (19)$$

Nun beweist man leicht analog wie in Hensel, Zahlentheorie, S. 306, daß die in der letzten Gleichung rechtsstehende binäre Form entweder $\mathfrak{p}$ als Teiler besitzt oder indefinit ist, d. h. sowohl Quadrate wie auch Nichtquadrate darstellt.

Wir nehmen nämlich an,

$$\varphi(x_1, x_2) = w_{\mathfrak{p}}^{a_1} x_1^2 + w_{\mathfrak{p}}^{a_2} x_2^2$$

enthalte $\mathfrak{p}$ nicht als Teiler. Dann ist nach Satz 1

$$\left[\frac{-w_{\mathfrak{p}}^{a_1+a_2}}{\mathfrak{p}}\right] = -1 = \left[\frac{-\tau_{\mathfrak{p}}}{\mathfrak{p}}\right],$$

wenn wir für den Augenblick mit $\tau_{\mathfrak{p}}$ die Invariante von φ in $K(\mathfrak{p})$ bezeichnen. Nach Multiplikation von φ mit $w_{\mathfrak{p}}^{a_1}$ und nachfolgender Transformation können wir es in der normierten Form

$$\varphi_0 = x_1'^2 + \tau_{\mathfrak{p}} x_2'^2$$

annehmen. Wir machen nun die Annahme, φ_0 stelle lauter Nichtreste dar. Alle Nichtreste sind kongruent *mod P* den ungeraden Potenzen von $w_{\mathfrak{p}}$. Wir erhielten also auch Nichtreste, wenn wir für x_1' der Reihe nach die Werte $w_{\mathfrak{p}}^0$, $w_{\mathfrak{p}}$, $w_{\mathfrak{p}}^2$, ..., $w_{\mathfrak{p}}^{\frac{p^\pi - 3}{2}}$ einsetzen würden. Dann durchläuft $x_1'^2$ alle inkongruenten Reste $\varrho_1, \varrho_2, \ldots, \varrho_{\frac{p^\pi - 1}{2}}$ und da alle $\frac{p^\pi - 1}{2}$ Funktionen $\varrho_i + \tau_{\mathfrak{p}}$ *mod P* inkongruent sind, erhalten wir, wenn wir $x_2' = 1$ setzen, die $\frac{p^\pi - 1}{2}$ Kongruenzen

$$\varrho_i + \tau_{\mathfrak{p}} \equiv \nu_i \ mod\ P \left(i = 1, \ldots, \frac{p^\pi - 1}{2}\right),$$

wo die ν_i das System der $\frac{p^\pi - 1}{2}$ Nichtreste *mod P* bedeuten sollen. Addieren wir alle Kongruenzen, so ergibt sich:

$$\sum \varrho_i + \frac{p^\pi - 1}{2} \tau_{\mathfrak{p}} \equiv \sum \nu_i \ mod\ P.$$

Nun zeigt man leicht ganz analog wie in der rationalen Zahlentheorie, daß $\Sigma \varrho_i \equiv \Sigma \nu_i \equiv 0 \ mod\ P$. Dann würde sich aber aus der letzten Kongruenz ergeben, daß

$$\frac{p^\pi - 1}{2} \tau_{\mathfrak{p}} \equiv 0 \ mod\ P,$$

$$\tau_{\mathfrak{p}} \equiv 0 \ mod\ P,$$

im Gegensatz zur Annahme, die wir über $\tau_\mathfrak{p}$ gemacht haben. Noch leichter widerlegt sich auf ähnlichem Wege die Annahme, daß φ_0 nur Reste darstellt. Damit ist aber der Satz bewiesen.

Enthält nun die binäre Teilform φ von f P als Teiler, so ist nach dem am Schluß von § 2 erwähnten Teilformenprinzip die Null auch durch f in $K(\mathfrak{p})$ darstellbar. Im anderen Falle ist nach vorigem die Gleichung (19) immer durch eine $\mathfrak{p}$-adische Funktion x_0 zu erfüllen. Die Lösung ist also in jedem Falle möglich. Zusammenfassend können wir also sagen, daß $\left(\frac{\alpha_1, \alpha_2}{\mathfrak{p}}\right) = +1$ immer dann ist, wenn α_1 und α_2 Einheiten *mod* P sind, oder

$$\left(\frac{w_\mathfrak{p}^{a_1}, w_\mathfrak{p}^{a_2}}{\mathfrak{p}}\right) = +1 \quad \ldots\ldots\ldots\ldots \quad (20)$$

Es sei jetzt wenigstens eins der α_1, α_2 durch P teilbar. Sind es beide, so kann man durch Multiplikation mit P und nachfolgende Transformation immer erreichen, daß nur ein Koeffizient durch P teilbar wird. Wir können demnach f jetzt von vornherein in der Form annehmen:

$$f(x_0, x_1, x_2) = -x_0^2 + w_\mathfrak{p}^{a_1} x_1^2 + w_\mathfrak{p}^{a_2} P x_2^2.$$

Ist $a_1 = 0$, so stellt offenbar schon die binäre Teilform $-x_0^2 + x_1^2$ die Null dar. Wir können also $a_1 = 1$ voraussetzen. Betrachten wir jetzt $f = 0$ als Kongruenz *mod* P, so wird

$$-x_0^2 + w_\mathfrak{p} x_1^2 \equiv 0 \ \textit{mod}\ P,$$
$$\left(\frac{x_0}{x_1}\right)^2 \equiv w_\mathfrak{p} \ \textit{mod}\ P.$$

Nun kann aber $w_\mathfrak{p}$ niemals quadratischer Rest *mod* P sein. Es ergibt sich in diesem Falle daher für das Symbol der Wert -1. Zusammenfassend können wir also die Formel anmerken:

$$\left(\frac{w^{a_1}, w^{a_2} P}{\mathfrak{p}}\right) = \left[\frac{w^{a_1}}{\mathfrak{p}}\right] \quad \ldots\ldots\ldots \quad (21)$$

Zur schnellen Berechnung des Symbols wollen wir noch die sich leicht ergebende Formel anmerken:

$$\left(\frac{w^{a_1} P, w^{a_2} P}{\mathfrak{p}}\right) = \left(\frac{-w^{a_1+a_2}, w^{a_1} P}{\mathfrak{p}}\right) = \left[\frac{-w^{a_1+a_2}}{\mathfrak{p}}\right] \quad \ldots \quad (22)$$

Wir kommen jetzt zu $K(\mathfrak{p}_\infty)$. Hier dürfen wir f in der folgenden allgemeinsten Form annehmen:

$$f(x_0, x_1, x_2) = -x_0^2 + g^{a_1} t^{b_1} x_1^2 + g^{a_2} t^{b_2} x_2^2$$
$$(a_1, a_2, b_1, b_2 \text{ gleich } 0 \text{ oder } 1).$$

Ist zunächst $b_1 = b_2 = 0$, so hat f die Form:

$$f = -x_0^2 + g^{a_1} x_1^2 + g^{a_2} x_2^2.$$

Ist wenigstens noch etwa $a_1 = 0$, so sieht man sofort, daß die Darstellung der Null immer möglich ist. Es bleibt also nur noch der Fall zu betrachten, daß $a_1 = a_2 = 1$ ist, also f die Form hat

$$f = -x_0^2 + g x_1^2 + g x_2^2.$$

Hier hat man die beiden Fälle $p = 4n + 1$ und $p = 4n + 3$ zu unterscheiden. Ist $p = 4n + 1$, also -1 quadratischer Rest *mod* p, so sieht man leicht ein, daß schon die binäre Teilform $g x_1^2 + g x_2^2$ die Null darstellt. Ist dagegen $p = 4n + 3$, so setze man $x_1 = x_2 = 1$, wenn $p = 8n + 3$, und erhält aus $f = 0$ die Gleichung $x_0^2 = 2g$, die offenbar lösbar ist, da $\left(\frac{2}{p}\right) = -1$ ist. Ist dagegen $p = 8n + 7$, so kann man immer eine Primzahl q von der Form $4n + 1$ in der Darstellung $q = x_1'^2 + x_2'^2$ so finden, daß $\left(\frac{q}{p}\right) = -1$ wird. Setzt man dann $x_1 = x_1'$, $x_2 = x_2'$, so folgt aus $f = 0$ die andere Gleichung $x_0^2 = g q$, die dann auch in diesem Falle lösbar wird. Zusammenfassend können wir also die Formel anmerken:

$$\left(\frac{g^{a_1}, g^{a_2}}{\mathfrak{p}_\infty}\right) = +1 \quad \ldots\ldots\ldots\ldots \quad (23)$$

Ist zweitens wenigstens eins der b_1, b_2 gleich 1, so kann man wie vorher in $K(\mathfrak{p})$ f immer in die Form transformiert annehmen:

$$f = -x_0^2 + g^{a_1} x_1^2 + g^{a_2} t x_2^2,$$

wo nur ein Koeffizient durch t teilbar ist. Ist $a_1 = 0$, so ist $f = 0$ offenbar lösbar. Wir wollen also $a_1 = 1$ voraussetzen. Wir setzen an:

$$\begin{aligned} x_0 &= p_l t^l + p_{l-1} t^{l-1} + \cdots \quad (p_l \neq 0) \\ x_1 &= q_m t^m + q_{m-1} t^{m-1} + \cdots \quad (q_m \neq 0) \\ x_2 &= r_n t^n + r_{n-1} t^{n-1} + \cdots \quad (r_n \neq 0). \end{aligned}$$

Nun kann der Grad n von x_2 nicht größer oder gleich der größeren der beiden ganzen Zahlen l und m sein, da sonst in $g^{a_2} t x_2^2$ das Glied höchsten Grades von f vorkommen würde, das sich nicht wegheben könnte, so daß also auch $f = 0$ unmöglich wäre. Es muß also jedenfalls sein:

$$n < \mathrm{Max}\,(l, m).$$

Es sind also nur die folgenden fünf Fälle zu betrachten:

1. $l > m > n$.
2. $l = m > n$.
3. $m > l > n$.
4. $l > n \geqq m$.
5. $m > n \geqq l$.

Im 1. Falle hebt sich das Glied $-p_l^3 t^{2l}$ nicht fort. Im 2. müßte offenbar die Summe der Koeffizienten der höchsten Potenzen in den beiden ersten Gliedern von f kongruent $0 \mod p$ werden, oder

$$-p_l^2 + g\, q_m^2 \equiv 0 \mod p,$$
$$g\, q_m^2 \equiv p_l^2 \mod p,$$

was aber unmöglich ist, da links ein Nichtrest, rechts ein Rest steht. Im 3. würde sich das Glied $g\, q_m^3 t^{2m}$, im 4. das Glied $-p_l^2 t^{2l}$, im 5. das Glied $g\, q_m^2 t^{2m}$ nicht wegheben. Zusammenfassend können wir also die Formel anmerken:

$$\left\{\frac{g^{a_1}, g^{a_2} t}{\mathfrak{p}_\infty}\right\} = \left(\frac{g^{a_1}}{p}\right) = \left[\frac{g^{a_1}}{\mathfrak{p}_\infty}\right] \quad \ldots\ldots\ldots \quad (24)$$

wo $\left(\frac{g^{a_1}}{p}\right)$ das gewöhnliche Legendresche Symbol der rationalen Zahlentheorie bedeutet. Hervorzuheben ist die formale Analogie der Auswertungsregeln in $K(\mathfrak{p})$ und $K(\mathfrak{p}_\infty)$. Als besonders interessant mag noch der Spezialfall angemerkt werden:

$$\left\{\frac{1, \alpha_2}{\mathfrak{p}}\right\} = \left\{\frac{\alpha_1, 1}{\mathfrak{p}}\right\} = +1 \quad \ldots\ldots\ldots \quad (25)$$

der sowohl für $\mathfrak{p} = (P)$, wie auch für $\mathfrak{p} = \mathfrak{p}_\infty$ gilt.

Mit Hilfe dieser Auswertungsregeln beweisen wir jetzt den äußerst wichtigen Zerlegungssatz für das Symbol. Er lautet:

Für drei beliebige Funktionen $\alpha_1, \alpha_2', \alpha_2''$ besteht in jedem Körper $K(\mathfrak{p})$ die Gleichung:

$$\left\{\frac{\alpha_1, \alpha_2' \alpha_2''}{\mathfrak{p}}\right\} = \left\{\frac{\alpha_1, \alpha_2'}{\mathfrak{p}}\right\} \left\{\frac{\alpha_1, \alpha_2''}{\mathfrak{p}}\right\} \quad \ldots\ldots\ldots \quad (26)$$

neben ihr auf Grund des Vertauschungsgesetzes natürlich auch die andere:

$$\left\{\frac{\alpha_1' \alpha_1'', \alpha_2}{\mathfrak{p}}\right\} = \left\{\frac{\alpha_1', \alpha_2}{\mathfrak{p}}\right\} \left\{\frac{\alpha_1'', \alpha_2}{\mathfrak{p}}\right\} \quad \ldots\ldots\ldots \quad (26')$$

Diese Formeln sind ihrem Inhalt nach identisch mit dem folgenden schönen und einfachen Satze[1]):

Sind $\alpha_1, \alpha_2, \alpha_3$ drei beliebige Funktionen, für die die Beziehung

$$\alpha_1 \alpha_2 \alpha_3 = 1 \text{ in } K(\mathfrak{p})$$

besteht, so gilt immer die Gleichung:

$$\left\{\frac{\delta, \alpha_1}{\mathfrak{p}}\right\} \left\{\frac{\delta, \alpha_2}{\mathfrak{p}}\right\} \left\{\frac{\delta, \alpha_3}{\mathfrak{p}}\right\} = +1 \quad \ldots\ldots\ldots \quad (27)$$

für ein beliebiges δ.

In der Tat folgt ja aus dieser Gleichung durch Multiplikation mit $\left\{\frac{\delta, \alpha_3}{\mathfrak{p}}\right\}$:

$$\left\{\frac{\delta, \alpha_1}{\mathfrak{p}}\right\} \left\{\frac{\delta, \alpha_2}{\mathfrak{p}}\right\} = \left\{\frac{\delta, \alpha_3}{\mathfrak{p}}\right\} = \left\{\frac{\delta, \frac{1}{\alpha_1 \alpha_2}}{\mathfrak{p}}\right\} = \left\{\frac{\delta, \frac{(\alpha_1 \alpha_2)^2}{\alpha_1 \alpha_2}}{\mathfrak{p}}\right\} = \left\{\frac{\delta, \alpha_1 \alpha_2}{\mathfrak{p}}\right\}.$$

Umgekehrt folgt durch zweimalige Anwendung von (26)

$$\left\{\frac{\delta, \alpha_1}{\mathfrak{p}}\right\} \left\{\frac{\delta, \alpha_2}{\mathfrak{p}}\right\} \left\{\frac{\delta, \alpha_3}{\mathfrak{p}}\right\} = \left\{\frac{\delta, \alpha_1 \alpha_2 \alpha_3}{\mathfrak{p}}\right\} = \left\{\frac{\delta, 1}{\mathfrak{p}}\right\} = +1$$

nach (25). Wir brauchen also nur die Richtigkeit von (27) nachzuweisen.

Dabei müssen wir die Fälle unterscheiden, daß $\delta, \alpha_1, \alpha_2, \alpha_3$ gerade oder ungerade Ordnungszahlen in $K(\mathfrak{p})$ bzw. geraden oder ungeraden Grad in $K(\mathfrak{p}_\infty)$ besitzen. Anzumerken ist noch, daß von den drei Funktionen $\alpha_1, \alpha_2, \alpha_3$ keine oder zwei von ungerader Ordnung bzw. ungeradem Grad sind, da ihr Produkt gleich 1 ist. Ferner ist: $(\alpha_{1\mathfrak{p}}\ \alpha_{2\mathfrak{p}}\ \alpha_{3\mathfrak{p}})_{\mathfrak{p}} = (\alpha_{1\mathfrak{p}_\infty}\ \alpha_{2\mathfrak{p}_\infty}\ \alpha_{3\mathfrak{p}_\infty})_{\mathfrak{p}_\infty} = +1$.

Ist nun zunächst δ von gerader Ordnung in $K(\mathfrak{p})$ bzw. geradem Grad in $K(\mathfrak{p}_\infty)$, und nehmen wir auch $\alpha_1, \alpha_2, \alpha_3$ alle ebenfalls von gerader Ordnungszahl bzw. geradem Grad an, so ist (27) richtig, denn sowohl in $K(\mathfrak{p})$ wie in $K(\mathfrak{p}_\infty)$ folgt aus (20) und (23), daß alle Symbole gleich $+1$, also auch die ganze linke Seite gleich $+1$ ist. Ist dagegen unter der gleichen Voraussetzung über δ α_1 von gerader, α_2 und α_3 aber von ungerader Ordnungszahl bzw. Grad, so wird in (27) das zweite und dritte Symbol gleich $\left[\frac{\delta_\mathfrak{p}}{\mathfrak{p}}\right]$ einschließlich $\mathfrak{p} = \mathfrak{p}_\infty$, so daß (27) übergeht in die richtige Gleichung:

$$(+1)\left[\frac{\delta_\mathfrak{p}}{\mathfrak{p}}\right]\left[\frac{\delta_\mathfrak{p}}{\mathfrak{p}}\right] = +1.$$

---

[1]) Vgl. K. Hensel, Zahlentheorie, S. 318 ff.

Ist jetzt aber δ von ungerader Ordnung bzw. ungeradem Grad, $\alpha_1, \alpha_2, \alpha_3$ aber zunächst alle von gerader Ordnung bzw. Grad, so geht (27) über in

$$\left[\frac{\alpha_{1\mathfrak{p}}}{\mathfrak{p}}\right]\left[\frac{\alpha_{2\mathfrak{p}}}{\mathfrak{p}}\right]\left[\frac{\alpha_{3\mathfrak{p}}}{\mathfrak{p}}\right] = \left[\frac{\alpha_{1\mathfrak{p}}\,\alpha_{2\mathfrak{p}}\,\alpha_{3\mathfrak{p}}}{\mathfrak{p}}\right] = +1.$$

Behält schließlich δ ungerade Ordnungszahl bzw. ungeraden Grad, während α_1 von gerader, α_2 und α_3 aber von ungerader Ordnung bzw. Grad vorausgesetzt werden, so geht (27) nach (21) und (22) bzw. nach (24) über in

$$\left[\frac{\alpha_{1\mathfrak{p}}}{\mathfrak{p}}\right]\left[\frac{-\alpha_{2\mathfrak{p}}\,\delta_{\mathfrak{p}}}{\mathfrak{p}}\right]\left[\frac{-\alpha_{3\mathfrak{p}}\,\delta_{\mathfrak{p}}}{\mathfrak{p}}\right] = \left[\frac{\alpha_{1\mathfrak{p}}\,\alpha_{2\mathfrak{p}}\,\alpha_{3\mathfrak{p}}\,\delta_{\mathfrak{p}}^2}{\mathfrak{p}}\right] = +1,$$

womit unser Zerlegungssatz dann vollständig bewiesen ist.

Wir beweisen noch den für das Folgende wichtigen Produktsatz für das Symbol:

Sind α_1, α_2 beliebige Größen aus K, so besteht die Gleichung

$$\prod_i \left\{\frac{\alpha_1, \alpha_2}{\mathfrak{p}_i}\right\} = +1, \quad \ldots\ldots\ldots\ldots \quad (28)$$

wo das Produkt über alle Primideale $\mathfrak{p}$ einschließlich $\mathfrak{p} = \mathfrak{p}_\infty$ zu erstrecken ist. Der Satz ist gleichbedeutend damit, daß die ternäre Form $f = -x_0^2 + \alpha_1 x_1^2 + \alpha_2 x_2^2$ nur eine endliche, und zwar gerade Anzahl von Nichtteilern enthält.

Für den Beweis genügt es offenbar, α_1 und α_2 als quadratische Kerne in K anzunehmen. Ist nun etwa $\alpha_1 = g^{a_1} P_{11} P_{12} \ldots P_{1m}$, $\alpha_2 = g^{a_2} P_{21} \ldots P_{2n}$, wo P_{ik} Primfunktionen, so kann man jedes Symbol $\left\{\frac{\alpha_1, \alpha_2}{\mathfrak{p}}\right\}$ mit Hilfe des Zerlegungs- und Vertauschungssatzes so lange zerlegen, bis lauter Faktoren von einer der Formen $\left\{\frac{g^{a_1}, g^{a_2}}{\mathfrak{p}}\right\}$, $\left\{\frac{g^{a_1}, P_{2k}}{\mathfrak{p}}\right\}$, $\left\{\frac{P_{1k}, P_{2l}}{\mathfrak{p}}\right\}$ vorliegen. Der Satz wird also bewiesen sein, wenn der Beweis für jede dieser drei Symbolarten gelingt. Eine leichte Überlegung zeigt nun, daß es genügt, die folgenden vier Spezialfälle des Satzes zu beweisen, da der Satz in allen übrigen Fällen nach (25) von selbst erfüllt ist:

$$\prod_i \left\{\frac{g, g}{\mathfrak{p}_i}\right\}, \quad \prod_i \left\{\frac{g, P}{\mathfrak{p}_i}\right\}, \quad \prod_i \left\{\frac{P, P}{\mathfrak{p}_i}\right\}, \quad \prod_i \left\{\frac{P, Q}{\mathfrak{p}_i}\right\}.$$

Dabei bedeuten P und Q voneinander verschiedene Primfunktionen.

Beim ersten Produkt folgt aus den Auswertungsregeln (20) und (23) unmittelbar, daß alle einzelnen Symbole, also auch das ganze Produkt gleich $+1$ sind.

Im zweiten Produkt braucht nur das Teilprodukt $\left\{\frac{g, P}{\mathfrak{p}}\right\} \left\{\frac{g, P}{\mathfrak{p}_\infty}\right\}$ betrachtet zu werden, wo $\mathfrak{p} = (P)$ gesetzt ist. Denn ist $\mathfrak{q} \neq (P)$, so muß der $\mathfrak{q}$-adische Kern von P notwendig zu $\mathfrak{q}$ teilerfremd sein und dann folgt nach den Auswertungsregeln für das Symbol der Wert $+1$. Nun folgt für $\left\{\frac{g, P}{\mathfrak{p}}\right\}$ nach den Auswertungsregeln:

$$\left\{\frac{g, P}{\mathfrak{p}}\right\} = \left[\frac{g}{P}\right] = \left(\frac{g}{p}\right)^{\pi} \quad (\pi = \text{Grad von } P),$$

der letztere Wert nach dem Ergänzungssatz von Herrn Artin. Es ist aber auch

$$\left\{\frac{g, P}{\mathfrak{p}_\infty}\right\} = \left(\frac{g}{p}\right)^{\pi},$$

denn nach (23) und (24) hat dies Symbol den Wert $+1$, wenn π gerade, also $P_{\mathfrak{p}_\infty} = 1$ ist, und nur dann den Wert -1, wenn π ungerade, also $P_{\mathfrak{p}_\infty} = t$ ist, in Übereinstimmung mit der rechten Seite, die man auch gleich $(-1)^{\pi}$ setzen kann. Damit wird aber auch das betrachtete Teilprodukt gleich $+1$ und unser Satz ist für diesen Spezialfall bewiesen.

Beim dritten Produkt braucht nur das Teilprodukt $\left\{\frac{P, P}{\mathfrak{p}}\right\} \left\{\frac{P, P}{\mathfrak{p}_\infty}\right\}$ betrachtet zu werden, da nach der beim zweiten Produkt gemachten Bemerkung alle anderen Faktoren gleich $+1$ sind. Nun ist $\left\{\frac{P, P}{\mathfrak{p}}\right\}$ $= \left\{\frac{-1, P}{\mathfrak{p}}\right\} = \left[\frac{-1}{\mathfrak{p}}\right] = \left(\frac{-1}{p}\right)^{\pi}$, aber auch $\left\{\frac{P, P}{\mathfrak{p}_\infty}\right\} = \left(\frac{-1}{p}\right)^{\pi}$, da als $\mathfrak{p}_\infty$-adische Kerne von P nur 1 und t in Frage kommen, 1 in dem Falle, wo π gerade, t, wo π ungerade. Im ersten Falle ist das Symbol gleich $+1$, im zweiten gleich $\left\{\frac{-1, t}{\mathfrak{p}_\infty}\right\} = \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)^{\pi}$, also das betrachtete Teilprodukt gleich $+1$, was zu beweisen war.

Beim vierten Produkt endlich braucht nur das Teilprodukt $\left\{\frac{P, Q}{\mathfrak{p}}\right\} \left\{\frac{P, Q}{\mathfrak{q}}\right\} \left\{\frac{P, Q}{\mathfrak{p}_\infty}\right\}$ untersucht zu werden, wo $\mathfrak{p} = (P)$, $\mathfrak{q} = (Q)$ gesetzt ist, alle andern Faktoren werden nach vorigem gleich $+1$. Nun ist $\left\{\frac{P, Q}{\mathfrak{p}}\right\} = \left[\frac{Q}{\mathfrak{p}}\right]$, $\left\{\frac{P, Q}{\mathfrak{q}}\right\} = \left[\frac{P}{\mathfrak{q}}\right]$, $\left\{\frac{P, Q}{\mathfrak{p}_\infty}\right\} = \left(\frac{-1}{p}\right)^{\varkappa\pi}$, ($\varkappa$ = Grad

von Q), wie eine leichte Betrachtung der Grade von P und Q zeigt. Nach dem von Herrn Artin bewiesenen Reziprozitätsgesetz[1]) gilt aber in K:

$$\left[\frac{P}{\mathfrak{q}}\right]\left[\frac{Q}{\mathfrak{p}}\right] = \left(\frac{-1}{p}\right)^{\varepsilon\tau}.$$

und damit ergibt sich auch für dies Teilprodukt der Wert -1. Damit ist dann der Beweis des Produktsatzes in allen seinen Teilen geliefert.

§ 6. Darstellbarkeit in $K(\mathfrak{p})$ durch binäre Formen.

Liegt die binäre Form $f(x_1, x_2) = \alpha_1 x_1^2 + \alpha_2 x_2^2$ vor und soll die Funktion μ in $K(\mathfrak{p})$ durch f in $K(\mathfrak{p})$ darstellbar sein, also

$$\mu = \alpha_1 x_1^2 + \alpha_2 x_2^2 \quad \ldots\ldots\ldots\ldots \quad (29)$$

gelten, so muß die Null durch die ternäre Form

$$-\mu x_0^2 + \alpha_1 x_1^2 + \alpha_2 x_2^2$$

darstellbar sein. Dazu ist aber nach § 4 erforderlich, daß

$$\left\{\frac{\alpha_1 \mu, -\alpha_1 \alpha_2}{\mathfrak{p}}\right\} = -1 \quad \ldots\ldots\ldots\ldots \quad (30)$$

wird (einschließlich $\mathfrak{p} = \mathfrak{p}_\infty$). Aus (30) folgt aber nach dem Zerlegungssatz sofort die Gleichung:

$$\left\{\frac{\mu, -\alpha_1 \alpha_2}{\mathfrak{p}}\right\} = \left\{\frac{\alpha_1, -\alpha_1 \alpha_2}{\mathfrak{p}}\right\} \quad \ldots\ldots\ldots \quad (30')$$

Da $\left\{\frac{\alpha_1, -\alpha_1 \alpha_2}{\mathfrak{p}}\right\}$ eine feste, nur durch die Form f bestimmte rationale Einheit ist, ergibt sich aus (30′) sofort der

Satz 5: Zu jeder binären Form der Invariante $\delta_\mathfrak{p}$ gibt es eine Einheit $\check{c}_\mathfrak{p} = \check{c}_\mathfrak{p}(f)$, so daß f alle und nur die $\mathfrak{p}$-adischen Funktionen $\mu(\neq 0)$ in $K(\mathfrak{p})$ darstellt, für die

$$\left\{\frac{\mu, -\delta_\mathfrak{p}}{\mathfrak{p}}\right\} = \check{c}_\mathfrak{p} \quad \ldots\ldots\ldots\ldots \quad (31)$$

ist.

Die Einheit $\check{c}_\mathfrak{p}(f)$ ist demnach, ebenso wie $\delta_\mathfrak{p}$ und die Darstellbarkeit jedes μ durch f, invariant gegen $\mathfrak{p}$-adische Transformation von f. Sie berechnet sich durch

$$\check{c}_\mathfrak{p} = \left\{\frac{\alpha, -\delta_\mathfrak{p}}{\mathfrak{p}}\right\}, \quad \ldots\ldots\ldots\ldots \quad (32)$$

wo α irgend eine durch f darstellbare Funktion, z. B. α_1 oder α_2 ist.

[1]) Artin, § 15.

§ 7. Darstellbarkeit der Null in K durch ternäre Formen.

Der Fundamentalsatz (II) für $\mu = 0$ und $n = 3$ lautet:

Satz 6: Eine ternäre Form stellt die Null dann und nur dann in K dar, wenn sie sie in allen $K(\mathfrak{p})$ darstellt, d. h. wenn ihr System $(\hat{c}_\mathfrak{p})$ der Bedingung $\hat{c}_\mathfrak{p} \equiv +1$ genügt.

Beweis: Wegen der Invarianz der Darstellbarkeit der Null gegen Transformation und Multiplikation in K können wir die gegebene Form in der Normalform

$$f_0 = -x_0^2 + \alpha_1 x_1^2 + \alpha_2 x_2^2$$

ansetzen, wo α_1 und α_2 quadratische Kerne aus K sind, also ganze rationale Funktionen von t. Die Notwendigkeit der Bedingung leuchtet unmittelbar ein. Wir wollen demnach gleich voraussetzen, daß f_0 die Null in allen $K(\mathfrak{p})$ darstellt, daß demnach

$$\hat{c}_\mathfrak{p}(f_0) \equiv \left\{\frac{\alpha_1, \alpha_2}{\mathfrak{p}}\right\} \equiv +1$$

ist, und weisen dann nach, daß die Gleichung $f_0 = 0$ eine Lösung in K zuläßt. Wir wollen die Zahl $J = \mathrm{Max}[\mathfrak{Gr}(\alpha_1), \mathfrak{Gr}(\alpha_2)]$ den Index der Form f_0 nennen. Offenbar gilt $J \geqq 0$ ganz rational. Außerdem können wir ohne Einschränkung $0 \leqq \mathfrak{Gr}(\alpha_1) \leqq \mathfrak{Gr}(\alpha_2)$, also $J = \mathfrak{Gr}(\alpha_2)$ annehmen.

Ist nun zunächst $J = 0$, so muß $\alpha_1 = g^{a_1}$, $\alpha_2 = g^{a_2}$ (a_1, a_2 gleich 0 oder 1) sein. f_0 ist in diesem Falle also von der Form:

$$\bar{f}_0 = -x_0^2 + g^{a_1} x_1^2 + g^{a_2} x_2^2.$$

Daß diese Form aber in K immer eine Lösung besitzt, ist beim Beweis der Formel (23) schon mitbewiesen worden. Der Satz ist also nur noch für den Fall zu beweisen, daß $J \geqq 1$ ist. Er wird aber bewiesen sein, wenn wir zeigen können, daß sich in diesem Falle entweder eine Lösung direkt angeben oder doch f_0 durch Transformation und Multiplikation in eine Form f_0' so umwandeln läßt, daß der Index J' von f_0' kleiner wird als der von f_0. Auf f_0' kann man dann wieder dasselbe Verfahren anwenden und gelangt so schließlich auf den Index $J = 0$, für den der Satz bereits bewiesen ist.

Nun folgt aus der Voraussetzung $\hat{c}_\mathfrak{p} \equiv +1$ die Existenz einer Lösung in K der Kongruenz

$$\lambda^2 \equiv \alpha_1 \bmod \alpha_2 \quad \ldots\ldots\ldots\ldots \quad (33)$$

Denn diese Kongruenz ist lösbar:

1. für alle in α_1 nicht enthaltenen, nach Voraussetzung notwendig einfachen, Primfaktoren Q_i von α_2 wegen

$$\left(\frac{\alpha_1, \alpha_2}{q_i}\right) = \left[\frac{\alpha_1}{q_i}\right] = +1;$$

2. für alle gemeinsamen Teiler P_k von α_1 und α_2 durch die Nullklasse *mod* P_k.

Der in α_2 etwa noch vorkommende Faktor g tut der Möglichkeit der Kongruenz keinen Abbruch. Da nun alle Primfaktoren von α_2 voneinander verschieden sind, lassen sich die Lösungen der Teilkongruenzen (analog wie im entsprechenden Falle der rationalen Zahlentheorie) zu einer Lösung λ der Kongruenz (33) zusammenfassen.

Wir wählen nun die Funktion λ (die auch verschwinden kann) aus ihrer Restklasse *mod* α_2 so aus, daß $\mathfrak{Gr}(\lambda) < \mathfrak{Gr}(\alpha_2)$, was immer möglich ist, und wollen dann setzen:

$$\lambda^2 - \alpha_1 = \alpha_2 \alpha_2', \quad \ldots\ldots\ldots\ldots (33')$$

wo α_2' eine ganze Funktion aus K ist. Ist nun $\alpha_2' = 0$ oder ein Quadrat in K, so stellt schon diese Gleichung eine nicht identische Lösung von $f_0 = 0$ dar. Ist dies aber nicht der Fall, so erhält man aus f_0 durch die Substitution

$$\left.\begin{aligned} x_0' &= \lambda x_0 + \alpha_1 x_1 + 0\, x_2 \\ x_1' &= x_0 + \lambda x_1 + 0\, x_2 \\ x_2' &= 0\, x_0 + 0\, x_1 + \alpha_2' x_2 \end{aligned}\right\} \quad \ldots\ldots\ldots (34)$$

mit der Determinante $(\lambda^2 - \alpha_1)\alpha_2' = \alpha_2 \alpha_2'^2 \not\equiv 0$ und anschließende Division mit $\alpha_2 \alpha_2' (\not\equiv 0)$ leicht die neue Form:

$$f_0' = -x_0'^2 + \alpha_1 x_1'^2 + \alpha_2' x_2'^2 \quad \ldots\ldots\ldots (35)$$

Wir wollen nun durch l, ν_1, ν_2, ν_2' bzw. die Grade von $\lambda, \alpha_1, \alpha_2, \alpha_2'$ bezeichnen. Dann folgt aber aus (33'):

$$\mathrm{Max}(2l, \nu_1) - \nu_2 \geqq \nu_2' \quad (l < \nu_2) \quad \ldots\ldots\ldots (36)$$

Ist nun

1. $\nu_1 = \nu_2$ und

a) $2l > \nu_1 = \nu_2$, so folgt aus (36) bei Berücksichtigung der rechtsstehenden Ungleichung:

$$2l - \nu_2 \geqq \nu_2'; \quad \nu_2' < \nu_2; \quad \text{für}$$

b) $2l \leqq \nu_1 = \nu_2$ folgt ebenso

$$\nu_1 - \nu_2 \geqq \nu_2'; \quad \nu_2' \leqq 0, \text{ d. h. } \nu_2' = 0.$$

Immer ist es also, wenn $\nu_1 = \nu_2$, möglich, durch die Transformation (34) eine Form f_0' aus f_0 zu erhalten, bei der $\mathfrak{Gr}(\alpha_1) \neq \mathfrak{Gr}(\alpha_2)$. Diesem Falle wenden wir uns nun zu und nehmen also an:

2. $\nu_1 < \nu_2$.

Da $\nu_2' \geqq 0$, muß jetzt $\mathrm{Max}(2l, \nu_1) = 2l \geqq \nu_2$ werden. Dann folgt aus (36): $2l - \nu_2 \geqq \nu_2'$ und

$$\nu_2' < \nu_2.$$

In diesem Falle wird also tatsächlich der Index kleiner.

Durch fortgesetzte Substitutionen (34) kann man also entweder sofort den Index der Form erniedrigen, oder, wenn die Grade der Koeffizienten gleich sind, eine Form mit gleichem Index, aber verschiedenen Graden der Koeffizienten erhalten, so daß eine Transformation (34) dieser neuen Form nun eine wirkliche Erniedrigung des Index zur Folge hat. Damit ist aber Satz 6 vollständig bewiesen.

§ 8. Darstellbarkeit in K durch binäre Formen.

Aus Satz 6 folgt nach (IV) sofort die Gültigkeit des Fundamentalsatzes (II) für die Darstellbarkeit beliebiger Funktionen μ durch binäre Formen in K. Aus den Darstellbarkeitskriterien des Satzes 5 für die einzelnen $K(\mathfrak{p})$ ergeben sich dann die folgenden Kriterien für die Darstellbarkeit in K durch binäre Formen:

Satz 7: Zu einer binären Form der Invariante δ gibt es ein auf alle $\mathfrak{p}$ erstrecktes System von Einheiten $(\check{c}_\mathfrak{p}) = (\check{c}_\mathfrak{p}(f))$, so daß f alle und nur die Funktionen μ $(\neq 0)$ aus K in K darstellt, für die

$$\left\{\frac{\mu, -\delta}{\mathfrak{p}}\right\} \equiv \check{c}_\mathfrak{p} \quad \ldots\ldots\ldots\ldots \quad (31')$$

ist.

Das System $(\check{c}_\mathfrak{p}(f))$ ist demnach, ebenso wie δ und die Darstellbarkeit jedes μ in K durch f, invariant gegen Transformation von f in K. Es berechnet sich durch

$$\check{c}_\mathfrak{p} \equiv \left\{\frac{\alpha, -\delta}{\mathfrak{p}}\right\},$$

wo α irgend eine durch f darstellbare Funktion in K, z. B. der Koeffizient eines rein quadratischen Gliedes von f ist.

Aus Satz 7 ergibt sich auch noch, daß einzig und allein für $\delta = 1$, wenn $p = 4n + 1$, bzw. $\delta = g$, wenn $p = 4n + 3$, alle Funktionen aus K in K darstellbar sind. Denn für jedes andere δ

ist $-\delta$ in mindestens einem der $K(\mathfrak{p})$ Nichtquadrat. Dann zeigt man aber leicht ähnlich wie in Hensel, Zahlentheorie, Kap. XII, S. 328, daß nicht alle $\mathfrak{p}$-adischen Funktionen den Bedingungen von Satz 7 genügen, so daß es sicher Funktionen μ in K gibt, die in diesen $K(\mathfrak{p})$ nicht darstellbar sind, also auch nicht in K. Dies folgt leicht auf die folgende Art. Mittels des Zerlegungsgesetzes ergibt sich allgemein:

$$\left(\frac{\mu, \Delta}{\mathfrak{p}}\right) = \left(\frac{w_{\mathfrak{p}}^{a'} P^{b'}, w_{\mathfrak{p}}^{a} P^{b}}{\mathfrak{p}}\right)$$
$$= \left(\frac{w_{\mathfrak{p}}^{a'}, w_{\mathfrak{p}}^{a}}{\mathfrak{p}}\right)\left(\frac{w_{\mathfrak{p}}^{a'}, P^{b}}{\mathfrak{p}}\right)\left(\frac{P^{b'}, w_{\mathfrak{p}}^{a}}{\mathfrak{p}}\right)\left(\frac{P^{b'}, P^{b}}{\mathfrak{p}}\right)$$

für $\mathfrak{p} = (P)$, bzw. für $\mathfrak{p} = \mathfrak{p}_\infty$:

$$\left(\frac{\mu, \Delta}{\mathfrak{p}_\infty}\right) = \left(\frac{g^{a'} t^{b'}, g^{a} t^{b}}{\mathfrak{p}_\infty}\right)$$
$$= \left(\frac{g^{a'}, g^{a}}{\mathfrak{p}_\infty}\right)\left(\frac{g^{a'}, t^{b}}{\mathfrak{p}_\infty}\right)\left(\frac{t^{b'}, g^{a}}{\mathfrak{p}_\infty}\right)\left(\frac{t^{b'}, t^{b}}{\mathfrak{p}_\infty}\right).$$

Aus den Auswertungsregeln folgt nun leicht:

$$\left.\begin{aligned}\left(\frac{\mu, \Delta}{\mathfrak{p}}\right) &= (-1)^{a'b + ab' + \frac{p-1}{2} \pi b b'} \quad \text{für } \mathfrak{p} = (P), \\ \left(\frac{\mu, \Delta}{\mathfrak{p}_\infty}\right) &= (-1)^{a'b + ab' + \frac{p-1}{2} b b'} \quad \text{für } \mathfrak{p} = \mathfrak{p}_\infty\end{aligned}\right\} \quad . \quad . \quad (37)$$

Aus dieser Darstellung erkennt man nun leicht, daß nur im Falle $a = b = 0$ die Symbole für beliebige μ sämtlich gleich $+1$ werden, d. h. Δ muß Quadrat sein, wenn die Null durch die ternäre Form $-x_0^2 + \mu x_1^2 + \Delta x_2^2$ in allen $K(\mathfrak{p})$ darstellbar sein soll. Setzt man jetzt für Δ den Wert $-\delta$ ein, so ergibt sich die obige Behauptung. Ist dagegen $\delta = 1$, wenn $p = 4n + 1$, bzw. $\delta = g$, wenn $p = 4n + 3$, so ist identisch $\left(\frac{\alpha, -\delta}{\mathfrak{p}}\right) \equiv \left(\frac{\alpha, 1}{\mathfrak{p}}\right) \equiv +1$, und die Bedingung von Satz 7 für jedes $\mu \neq 0$ aus K erfüllt. In Verbindung mit Satz 2 ergibt sich so der

Satz 8: Eine binäre Form stellt dann und nur dann alle Funktionen μ aus K und dann und nur dann auch die Null in K dar, wenn ihre Invariante δ gleich $+1$, wenn $p = 4n + 1$, bzw. gleich g, wenn $p = 4n + 3$.

C. Ternäre Formen.

§ 9. Darstellbarkeit der Null in $K(\mathfrak{p})$ durch quaternäre Formen.

Satz 9: Eine quaternäre Form stellt die Null in $K(\mathfrak{p})$ stets dar, wenn ihre Invariante $\delta_\mathfrak{p} \neq +1$ ist.

Zum Beweise können wir die quaternäre Form gleich in der Gestalt

$$f = x_0^2 + \alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2$$

annehmen, wo α_1, α_2, α_3 Kerne bedeuten. Es ist

$$\delta_\mathfrak{p} = (\alpha_1 \alpha_2 \alpha_3)_\mathfrak{p}.$$

1. $\mathfrak{p} = \mathfrak{p}_\infty$.

Wir setzen $\alpha_i = g^{a_i} t^{b_i} (i = 1, 2, 3;\ a_i, b_i = 0 \text{ oder } 1)$.

a) $\delta_{\mathfrak{p}_\infty} = g$.

In diesem Falle müssen die Kongruenzen bestehen:

$$a_1 + a_2 + a_3 \equiv 1 \ mod\ 2, \quad b_1 + b_2 + b_3 \equiv 0 \ mod\ 2,$$

oder in leicht verständlicher Symbolik:

$$(a) = (a_1, a_2, a_3) = (0, 0, 1) \text{ oder } = (1, 1, 1),$$
$$(b) = (b_1, b_2, b_3) = (0, 0, 0) \quad „ \quad = (0, 1, 1).$$

Bei passend gewählter Reihenfolge kommen nur die fünf durch ihre Koeffizienten angedeuteten Formentypen in Frage:

$$(1, 1, 1, g), \quad (1, g, g, g), \quad (1, 1, t, gt), \quad (1, g, t, t), \quad (1, g, gt, gt).$$

Jeder dieser fünf Typen ist von der Gestalt $\delta_1(1, 1) + \delta_2(1, g)$, wo δ_1 und δ_2 $\mathfrak{p}_\infty$-adische Kerne bedeuten. Da nun nach Satz 1 schon der binäre Typus $(1, 1)$ die Null darstellt, wenn $p = 4n + 1$, dagegen der Typus $(1, g)$ dasselbe leistet, wenn $p = 4n + 3$, so ist die Null in $K(\mathfrak{p}_\infty)$ durch jeden der fünf quaternären Typen für jedes p darstellbar, was zu beweisen war.

b) $\delta_{\mathfrak{p}_\infty} = t$ oder gleich gt.

Hier ist $(b) = (0, 0, 1)$ oder $(1, 1, 1)$, da $b_1 + b_2 + b_3 \equiv 1 \ mod\ 2$ werden muß. Im ersten Falle folgt aus

$$\left\{\frac{-\alpha_1, -\alpha_2}{\mathfrak{p}_\infty}\right\} = \left\{\frac{-g^{a_1}, -g^{a_2}}{\mathfrak{p}_\infty}\right\} = -1,$$

daß schon die x_0, x_1, x_2 entsprechende ternäre Teilform die Null in $K(\mathfrak{p}_\infty)$ darstellt. Im zweiten Falle ist

$$\left\{\frac{-\alpha_1\alpha_2, -\alpha_1\alpha_3}{\mathfrak{p}_\infty}\right\} = \left\{\frac{-g^{a_1+a_2}, -g^{a_1+a_3}}{\mathfrak{p}_\infty}\right\} = +1,$$

also stellt die x_1, x_2, x_3 entsprechende ternäre Teilform die Null dar, was zu beweisen war.

2. $\mathfrak{p} = (P)$.

Ersetzt man g durch $w_\mathfrak{p}$ und t durch P, so übersieht man leicht, daß auch in diesem Falle, wenn $\delta_\mathfrak{p} = w_\mathfrak{p}$, die entsprechenden fünf quaternären Formentypen aufgestellt werden können, die alle von der Gestalt $\delta_1(1,1) + \delta_2(1, w_\mathfrak{p})$ sind, wo δ_1 und δ_2 Kerne in $K(\mathfrak{p})$ bedeuten. Nun liefert Satz 1 für die Darstellbarkeit durch den Typus $(1,1)$ die Bedingung $\left(\frac{-1}{p}\right)^\pi = +1$, durch den Typus $(1, w_\mathfrak{p})$ aber die andere $\left(\frac{-1}{p}\right)^{\pi+1} = +1$. Man sieht, daß eine dieser Bedingungen immer erfüllt ist, daß also schon einer der binären Typen $(1,1)$ oder $(1, w_\mathfrak{p})$ die Null in $K(\mathfrak{p})$ darstellt. Für den zweiten Fall $\delta_\mathfrak{p} = w_\mathfrak{p} P$ bzw. $= P$ ergeben sich bei der eingangs erwähnten Substitution wegen der formalen Analogie der Auswertungsregeln unseres Symbols in $K(\mathfrak{p})$ bzw. in $K(\mathfrak{p}_\infty)$ dieselben Resultate wie unter 1. b). Damit ist der Satz dann aber vollständig bewiesen.

Wir können uns damit Satz 10 zuwenden, der in Verbindung mit Satz 9 die Darstellbarkeitskriterien der Null in den $K(\mathfrak{p})$ vollständig liefert:

Satz 10: Eine quaternäre Form f, deren Invariante $\delta_\mathfrak{p} = +1$ ist, stellt die Null in $K(\mathfrak{p})$ dann und nur dann dar, wenn in irgend einer (und damit in jeder) ihr in $K(\mathfrak{p})$ äquivalenten Form der besonderen Gestalt

$$f_0 = \alpha_0 x_0^2 + \varphi(x_1, x_2, x_3)$$

die Einheit $\hat{c}_\mathfrak{p}(\varphi) = +1$ ist.

Der Beweis verläuft ganz analog wie der des entsprechenden Satzes 11 in H. I. Ist $\hat{c}_\mathfrak{p}(\varphi) = +1$, so stellt schon die ternäre Teilform φ, also auch f_0 und f die Null in $K(\mathfrak{p})$ dar. Stellt umgekehrt f und somit f_0 die Null in $K(\mathfrak{p})$ dar, so gilt dies auch für die in $K(\mathfrak{p})$ äquivalente Form:

$$\bar{f}_0 = \alpha_0 x_0^2 + \varphi_0(x_1, x_2, x_3) = \alpha_0 x_0^2 + \alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2,$$

die durch Transformation von φ in eine in $K(\mathfrak{p})$ äquivalente reine Kernform φ_0 entsteht. Es besteht dann eine Gleichung

$$\mu = \alpha_0 x_0^2 + \alpha_1 x_1^2 = -\alpha_2 x_2^2 - \alpha_3 x_3^2, \quad \ldots\ldots \quad (38)$$

in der alle $x_i \neq 0$ angenommen werden dürfen. Ist $\mu = 0$, so darf man an seine Stelle ein anderes, von Null verschiedenes μ gesetzt denken, denn aus Satz 1 in Verbindung mit Satz 5 folgt leicht, daß

die beiden binären Formen alle $\mathfrak{p}$-adischen Funktionen darstellen, da ihre negativ genommenen Invarianten dann zur Funktionsklasse von $+1$ gehören. Zum Bestehen der beiden Gleichungen (38) für $\mu \neq 0$ ist aber nach Satz 5 notwendig, daß die beiden Bedingungen

$$\left\{\frac{\mu, -\alpha_0\alpha_1}{\mathfrak{p}}\right\} = \left\{\frac{\alpha_1, -\alpha_0\alpha_1}{\mathfrak{p}}\right\} \text{ und } \left\{\frac{\mu, -\alpha_2\alpha_3}{\mathfrak{p}}\right\} = \left\{\frac{-\alpha_2, -\alpha_2\alpha_3}{\mathfrak{p}}\right\} \quad (39)$$

für dies μ gleichzeitig bestehen. Nun ist nach Voraussetzung $\delta_\mathfrak{p} = +1$, also $\left[\frac{\delta_\mathfrak{p}}{\mathfrak{p}}\right] = \left[\frac{\alpha_0\alpha_1\alpha_2\alpha_3}{\mathfrak{p}}\right] = +1$ und daher $\left[\frac{-\alpha_0\alpha_1}{\mathfrak{p}}\right] = \left[\frac{-\alpha_2\alpha_3}{\mathfrak{p}}\right]$, und dasselbe gilt für $\mathfrak{p} = \mathfrak{p}_\infty$, d. h. $-\alpha_0\alpha_1$ und $-\alpha_2\alpha_3$ haben denselben Kern in $K(\mathfrak{p})$ und können in den Symbolen also durcheinander ersetzt werden. Die Bedingungen (39) können also nur dann ohne Widerspruch zusammen bestehen, wenn

$$\left\{\frac{\alpha_1, -\alpha_2\alpha_3}{\mathfrak{p}}\right\} = \left\{\frac{-\alpha_2, -\alpha_2\alpha_3}{\mathfrak{p}}\right\} \quad \ldots\ldots\ldots \quad (40)$$

gilt. Aus (40) folgt aber durch Multiplikation etwa mit dem rechts stehenden Symbol nach dem Zerlegungssatz:

$$\left\{\frac{\alpha_1, -\alpha_2\alpha_3}{\mathfrak{p}}\right\}\left\{\frac{-\alpha_2, -\alpha_2\alpha_3}{\mathfrak{p}}\right\} = \left\{\frac{-\alpha_1\alpha_2, -\alpha_2\alpha_3}{\mathfrak{p}}\right\} = +1 \quad (41)$$

d. h. aber, es ist $\hat{c}_\mathfrak{p}(\varphi_0) = \hat{c}_\mathfrak{p}(\varphi) = +1$, was zu beweisen war.

§ 10. Darstellbarkeit in $K(\mathfrak{p})$ durch ternäre Formen.

Aus den Sätzen 9 und 10 folgt jetzt sofort der

Satz 11: Eine ternäre Form der Invariante $\delta_\mathfrak{p}$ stellt in $K(\mathfrak{p})$ entweder alle $\mathfrak{p}$-adischen Funktionsklassen oder alle außer der $\mathfrak{p}$-adischen Funktionsklasse von $-\delta_\mathfrak{p}$ dar, je nachdem ihre Invariante $\delta_\mathfrak{p}$ den Wert $+1$ oder -1 hat.

Beweis: Nach (IV) werden durch eine ternäre Form $f(x_1, x_2, x_3)$ in $K(\mathfrak{p})$ alle und nur die Funktionsklassen μ dargestellt, für die die quaternäre Form

$$F = f(x_1, x_2, x_3) - \mu x_0^2$$

die Null in $K(\mathfrak{p})$ darstellt. Ist nun $\hat{c}_\mathfrak{p} = +1$, so stellt schon f nach Satz 4, also auch F für jede $\mathfrak{p}$-adische Funktionsklasse μ die Null in $K(\mathfrak{p})$ dar. Ist aber $\hat{c}_\mathfrak{p} = -1$, so stellt F nach den Sätzen 9

und 10 die Null dann und nur dann in $K(\mathfrak{p})$ dar, wenn ihre Invariante $\Delta_\mathfrak{p} \neq +1$ ist, d. h. wegen

$$\left[\frac{\Delta_\mathfrak{p}}{\mathfrak{p}}\right] = \left[\frac{-\mu\delta_\mathfrak{p}}{\mathfrak{p}}\right], \text{ wenn } \left[\frac{\mu}{\mathfrak{p}}\right] \neq \left[\frac{-\delta_\mathfrak{p}}{\mathfrak{p}}\right],$$

also die $\mathfrak{p}$-adische Funktionsklasse von μ verschieden ist von der $\mathfrak{p}$-adischen Funktionsklasse von $-\delta_\mathfrak{p}$, was zu beweisen war.

Aus Satz 11 folgt speziell unter Berücksichtigung von Satz 4 der

Satz 12: Eine ternäre Form stellt dann und nur dann alle $\mathfrak{p}$-adischen Funktionen und dann und nur dann auch die Null in $K(\mathfrak{p})$ dar, wenn ihre Invariante $\hat{c}_\mathfrak{p} = +1$ ist.

§ 11. Darstellbarkeit der Null in K durch quaternäre Formen.

Der Fundamentalsatz (II) für $\mu = 0$, $n = 4$ lautet:

Satz 13: Eine quaternäre Form stellt die Null dann und nur dann in K dar, wenn sie sie in allen $K(\mathfrak{p})$ darstellt.

Beweis: Wir haben nur das „dann" des Satzes zu beweisen und können uns auf reine Kernformen in K beschränken. Wir können also die quaternäre Form gleich in der Gestalt

$$f_0 = \alpha_0 x_0^2 + \alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2$$

und zugleich annehmen, daß f_0 die Null in allen $K(\mathfrak{p})$ darstellt. Die α_i sind jetzt also Kerne in K. Dann besteht in jedem $K(\mathfrak{p})$ eine Gleichung

$$\mu_\mathfrak{p} = \alpha_0 x_0^2 + \alpha_1 x_1^2 = -\alpha_2 x_2^2 - \alpha_3 x_3^2,$$

in der man $\mu_\mathfrak{p}$ als $\mathfrak{p}$-adischen Kern voraussetzen und zugleich ebenso wie beim Beweise von Satz 10 ungleich Null annehmen darf. Unser Satz wird nun bewiesen sein, wenn wir zeigen können, daß sich ein $\mu \neq 0$ in K finden läßt, das durch die obigen beiden binären Formen in K darstellbar ist. Dann stellt f_0 die Null auch in K dar.

Es bezeichne im folgenden P_i jede Primfunktion, die in den α_k aufgeht. Ferner setzen wir:

$$\mu_{\mathfrak{p}_i} = w_{\mathfrak{p}_i}^{a_i} P_i^{b_i} \ (a_i, b_i = 0 \text{ oder } 1),$$
$$\mu_{\mathfrak{p}_\infty} = g^a t^b \qquad (a, b = 0 \text{ oder } 1).$$

Alle Funktionen μ aus K, die gleichzeitig den Bedingungen:

$$\left.\begin{aligned} \mu &\equiv w_{\mathfrak{p}_i}^{a_i} P_i^{b_i} \ mod\, P_i^{b_i+1} \\ \mu_{\mathfrak{p}_\infty} &= g^a t^b \end{aligned}\right\} \quad \ldots\ldots\ldots (42)$$

genügen, unterscheiden sich von jedem der vorher genannten $\mu_{\mathfrak{p}}$ nur um ein $\mathfrak{p}$-adisches Quadrat, sind also gleichzeitig in $K(\mathfrak{p}_\infty)$ und den $K(\mathfrak{p}_i)$ durch die beiden binären Formen darstellbar. Die Bedingungen lassen sich einfacher zusammenziehen in die folgenden:

$$\left.\begin{aligned} \mu &\equiv \prod_i P_i^{b_i} \ldots A \bmod \prod_i P_i^{b_i+1}, \\ \mu_{\mathfrak{p}_\infty} &= g^a t^b, \end{aligned}\right\} \quad \ldots\ldots\ldots (43)$$

wo A eine zu $\prod_i P_i$ prime ganze Funktion aus K darstellt. Wir bestimmen jetzt eine Primfunktion P durch die Kongruenz:

$$P \equiv g^{-a} A \bmod \prod_i P_i \ldots\ldots\ldots (44)$$

Dies ist nach Artin (a. a. O., S. 246) immer möglich, da $g^{-a}A$ zu $\prod_i P_i$ prim ist, und wir sind außerdem noch in der Lage, den Grad von P willkürlich wählen zu können, und zwar tun wir dies so, daß wir diesen Grad gerade wählen, wenn $b = 0$ und $\mathfrak{Gr}\left(\prod_i P_i^{b_i}\right)$ gerade oder $b = 1$ und $\mathfrak{Gr}\left(\prod_i P_i^{b_i}\right)$ ungerade, dagegen ungerade, wenn $b = 0$ und $\mathfrak{Gr}\left(\prod_i P_i^{b_i}\right)$ ungerade oder $b = 1$ und $\mathfrak{Gr}\left(\prod_i P_i^{b_i}\right)$ gerade. Dann genügt die ganze Funktion in K:

$$\mu = g^a \prod_i P_i^{b_i} P \ldots\ldots\ldots\ldots (45)$$

den beiden zu stellenden Bedingungen, ist also in $K(\mathfrak{p}_i)$ einschließlich $K(\mathfrak{p}_\infty)$ durch die beiden binären Formen darstellbar. Dasselbe gilt aber auch für die übrigen $K(\mathfrak{p})$. Denn die nach Satz 5 für die Darstellbarkeit von μ in $K(\mathfrak{p})$ notwendigen und hinreichenden Kriterien:

$$\left\{\frac{\mu, -\alpha_0\alpha_1}{\mathfrak{p}}\right\} = \left\{\frac{\alpha_0, -\alpha_0\alpha_1}{\mathfrak{p}}\right\} \text{ und } \left\{\frac{\mu, -\alpha_2\alpha_3}{\mathfrak{p}}\right\} = \left\{\frac{-\alpha_2, -\alpha_2\alpha_3}{\mathfrak{p}}\right\} \quad (46)$$

sind für die übrigen $\mathfrak{p}$ außer (P) von selbst erfüllt, da diese $\mathfrak{p}$ weder in μ noch in den α_i aufgehen, also alle Symbole nach (20) gleich $+1$ werden. Dann folgt aber aus (46) nach dem Produktsatz für unser Symbol, daß (46) auch für $\mathfrak{p} = (P)$ erfüllt sein muß. Dann ist aber μ nach Satz 7 durch die beiden binären Formen in K darstellbar und dadurch der Beweis von Satz 13 erbracht.

§ 12. Darstellbarkeit in K durch ternäre Formen.

Aus Satz 13 folgt nach (IV) sofort die Gültigkeit des Fundamentalsatzes (II) für die Darstellbarkeit beliebiger Funktionen μ aus K durch ternäre Formen. Insbesondere ergeben sich aus den Darstellbarkeitskriterien des Satzes 11 für die einzelnen $K(\mathfrak{p})$ die folgenden Kriterien für die Darstellbarkeit in K durch ternäre Formen:

Satz 14: Damit eine Funktion $\mu \neq 0$ aus K durch eine ternäre Form mit den Invarianten δ und $(\hat{c}_\mathfrak{p})$ in K darstellbar ist, ist notwendig und hinreichend, daß μ den Bedingungen

$$\left[\frac{\mu}{\mathfrak{p}}\right] \neq \left[\frac{-\delta}{\mathfrak{p}}\right] \text{ für } \hat{c}_\mathfrak{p} = -1 \quad \ldots\ldots\ldots \quad (47)$$

genügt, d. h. für keinen der (endlich vielen) Bereiche $K(\mathfrak{p})$, für die $\hat{c}_\mathfrak{p} = -1$ ist, zur $\mathfrak{p}$-adischen Funktionsklasse von $-\delta$ gehört.

Endlich ergibt sich aus Satz 13 sofort der

Satz 15: Eine ternäre Form stellt dann und nur dann alle Funktionen μ aus K und dann und nur dann auch die Null in K dar, wenn ihr Invariantensystem $(\hat{c}_\mathfrak{p})$ der Bedingung

$$\hat{c}_\mathfrak{p} \equiv +1 \quad \ldots\ldots\ldots\ldots \quad (48)$$

genügt.

D. n-äre Formen ($n \geqq 4$).

§ 13. Darstellbarkeit in $K(\mathfrak{p})$ durch n-äre ($n \geqq 4$) Formen.

Uns interessieren auch hier zunächst die Darstellbarkeitsbedingungen der Null in $K(\mathfrak{p})$. Sie werden gegeben durch den

Satz 16: Eine n-äre Form ($n \geqq 5$) stellt die Null in jedem $K(\mathfrak{p})$ einschließlich $K(\mathfrak{p}_\infty)$ dar.

Beweis: Es ist nur nötig, den Satz für $n = 5$ zu beweisen. Für ein größeres n folgt er dann aus dem Teilformenprinzip ohne weiteres. Auch hier genügt es, von einer reinen Form auszugehen. Sei also

$$f_0 = \alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 + \alpha_4 x_4^2 + \alpha_5 x_5^2$$

eine reine quinäre Form, wo die α_i Kerne in $K(\mathfrak{p})$. Entweder hat nun eine ihrer quaternären Teilformen eine von $+1$ verschiedene Invariante $\delta'_\mathfrak{p}$; dann stellt nach Satz 9 diese Teilform und somit f_0

die Null in $K(\mathfrak{p})$ dar. Oder aber die Invarianten aller fünf quaternären Teilformen von f_0 sind gleich $+1$. Dann folgt aus

$$\left[\frac{\alpha_1\alpha_2\alpha_3\alpha_4}{\mathfrak{p}}\right] = \left[\frac{\alpha_1\alpha_2\alpha_3\alpha_5}{\mathfrak{p}}\right] = \left[\frac{\alpha_1\alpha_2\alpha_4\alpha_5}{\mathfrak{p}}\right]$$
$$= \left[\frac{\alpha_1\alpha_3\alpha_4\alpha_5}{\mathfrak{p}}\right] = \left[\frac{\alpha_2\alpha_3\alpha_4\alpha_5}{\mathfrak{p}}\right] = +1,$$

daß

$$\left[\frac{\alpha_1}{\mathfrak{p}}\right] = \left[\frac{\alpha_2}{\mathfrak{p}}\right] = \left[\frac{\alpha_3}{\mathfrak{p}}\right] = \left[\frac{\alpha_4}{\mathfrak{p}}\right] = \left[\frac{\alpha_5}{\mathfrak{p}}\right],$$

so daß also f_0 einem Multiplum von

$$\bar{f}_0 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$$

in $K(\mathfrak{p})$ äquivalent ist. Man überzeugt sich sofort, daß diese Betrachtung genau ebenso auch für $\mathfrak{p} = \mathfrak{p}_\infty$ gilt. Es stellt aber schon die ternäre Teilform $x_1^2 + x_2^2 + x_3^2$, also auch $\bar{f}_0$ und f_0 die Null in $K(\mathfrak{p})$ dar, was zu beweisen war.

Aus diesem Satze ergeben sich wieder mittels der Schlußweise (IV) die Darstellbarkeitskriterien für von Null verschiedene Funktionen in $K(\mathfrak{p})$:

Satz 17: Eine n-äre Form ($n \geqq 4$) stellt in jedem $K(\mathfrak{p})$ alle von Null verschiedenen $\mathfrak{p}$-adischen Funktionen dar.

§ 14. Darstellbarkeit in K durch n-äre Formen ($n \geqq 4$).

Für die Darstellbarkeit der Null in K durch n-äre Formen ($n \geqq 5$) ergibt sich der Fundamentalsatz (II) in dem folgenden:

Satz 18: Eine n-äre Form ($n \geqq 5$) stellt die Null dann und nur dann in K dar, wenn sie sie in allen $K(\mathfrak{p})$ darstellt, d. h. in jedem Falle.

Zum Beweise können wir uns auf das „dann“ des Satzes und auf reine Kernformen in K beschränken. Stellt eine solche die Null in allen $K(\mathfrak{p})$ dar, und das tut sie nach Satz 16 immer, so wollen wir eine quinäre Teilform aus ihr herausgreifen, die dann nach Satz 16 ebenfalls die Null in allen $K(\mathfrak{p})$ darstellt. Diese quinäre Teilform sei:

$$f_0 = [\alpha_1 x_1^2 + \alpha_2 x_2^2] + [\alpha_3 x_3^2 + \alpha_4 x_4^2 + \alpha_5 x_5^2] = \varphi + \psi.$$

Zum Beweise unseres Satzes wird es dann genügen, zu zeigen, daß f_0 die Null in K darstellt.

Ebenso wie beim Beweise von Satz 13 läßt sich hier die Existenz einer Funktion

$$\mu = g^a \prod_i P_i^{b_i} P$$

beweisen, die für die Bereiche von $\mathfrak{p}_\infty$ und allen Teilern $\mathfrak{p}_i$ der a_k durch die beiden Formen φ und $-\psi$ darstellbar ist. Unter Benutzung des Produktsatzes für unser Symbol kann man ebenso wie dort beweisen, daß dies μ auch für die übrigen $\mathfrak{p}$ durch die binäre Form φ darstellbar ist, so daß μ nach Satz 7 durch φ auch in K dargestellt werden kann.

Bei der ternären Form $-\psi$ sind die Invarianten $\hat{c}_\mathfrak{p}$ für alle nicht in den Koeffizienten enthaltenen $\mathfrak{p}$ nach den Auswertungsregeln gleich $+1$. Dann stellt aber nach Satz 11 die Form $-\psi$ alle $\mathfrak{p}$-adischen Funktionen dieser $K(\mathfrak{p})$, also auch μ dar. Da dies alle noch übrigen $\mathfrak{p}$ sind, so wird also μ in allen $K(\mathfrak{p})$ durch $-\psi$ dargestellt, nach dem schon bewiesenen Fundamentalsatz (II) dann aber auch in K. Somit ist $f_0 = 0$ in K lösbar, was zu beweisen war.

Auf Grund des eben bewiesenen Satzes folgt nach dem in (IV) vorgenommenen Schluß sofort die Gültigkeit des Fundamentalsatzes für $\mu \neq 0$, $n \geqq 4$. Dieser ist damit restlos bewiesen. Als Kriterium für die Darstellbarkeit von Null verschiedener Funktionen in K formulieren wir noch den

Satz 19: Eine n-äre Form ($n \geqq 4$) stellt alle von Null verschiedenen Funktionen von K in K dar.

§ 15. Zusammenfassung.

Damit ist unsere eingangs gestellte Hauptfragestellung (I) nach den Darstellbarkeitskriterien für quadratische Formen in K vollständig beantwortet. Wir geben noch eine kurze Zusammenstellung der Resultate in tabellarischer Form:

1. Darstellbarkeit von Null verschiedener Funktionen μ in K.

n	Invarianten	Darstellbarkeitskriterien
1	δ	$\left[\frac{\mu}{\mathfrak{p}}\right] \equiv \left[\frac{\delta}{\mathfrak{p}}\right]$
2	δ, $(\check{c}_\mathfrak{p})$	$\left\{\frac{\mu, -\delta}{\mathfrak{p}}\right\} \equiv (\check{c}_\mathfrak{p})$
3	δ, $(\hat{c}_\mathfrak{p})$	$\left[\frac{\mu}{\mathfrak{p}}\right] \neq \left[\frac{-\delta}{\mathfrak{p}}\right]$ für $\hat{c}_\mathfrak{p} = -1$
4, 5 ...	δ	jedes $\mu \neq 0$

2. Darstellbarkeit der Null in K.

n	Invarianten	Darstellbarkeitskriterien
2	δ, $(\check{c}_\mathfrak{p})$	$\left[\frac{-\delta}{\mathfrak{p}}\right] \equiv +1$
3	δ, $(\hat{c}_\mathfrak{p})$	$\hat{c}_\mathfrak{p} \equiv +1$
4	δ, $\left(\hat{c}_\mathfrak{p}(\varphi)\right)$	$\hat{c}_\mathfrak{p}(\varphi) = +1$ für $\left[\frac{\delta}{\mathfrak{p}}\right] = +1$
5, 6 ...	δ	in allen Fällen